XIX Congreso Internacional de Derecho Penal. "*Sociedad de la Información y Derecho Penal*"
(Río de Janeiro, Brasil, 31 agosto - 6 septiembre 2014)
Asociación Internacional de Derecho Penal (AIDP-IAPL)

SECCIÓN II – DERECHO PENAL PARTE ESPECIAL

SOCIEDAD DE LA INFORMACIÓN Y DERECHO PENAL

INFORME GENERAL*

Emilio C. VIANO
Relator General

De acuerdo con el Estudio Integral sobre la Ciberdelincuencia (Borrador, 2013) de la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD), en 2011, alrededor del 33 por ciento de la población mundial, es decir unos 2,3 billones, puede acceder a Internet. Es importante destacar que casi dos terceras partes viven en países en desarrollo y casi la mitad son menores de 25 años de edad. La penetración rápida y universal de los servicios de banda ancha se refleja en la predicción de que en el año 2017, el setenta por ciento de la población del mundo será suscrito y para el 2020 la cantidad de dispositivos conectados en red será seis veces mayor que las personas. Está claro que para entonces será difícil de conceptualizar casi cualquier crimen que no deje evidencia electrónica conectada a una conexión de protocolo de Internet. Recientes revelaciones de interceptación masiva o al menos el registro de las comunicaciones electrónicas en los Estados Unidos, Europa y otras regiones del mundo por parte de Estados Unidos y otros países, creando una enorme base de datos de las comunicaciones y los movimientos y ubicaciones de las personas, nos dan una idea del alcance y ámbito del " valiente nuevo mundo" electrónico en el que estamos entrando. La ciberdelincuencia está creciendo de forma concomitante, exponencialmente según algunos. Esto es inevitable, dado el hecho de que las herramientas y modalidades electrónicas son cada vez más profundamente entretejidas con todas las comunicaciones y transacciones personales, profesionales, financieras, de cumplimiento de la ley, gubernamentales y comerciales. Mercados negros cibernéticos, robo de datos, recolección y venta de información personal y financiera, la creación y distribución de software malicioso, la gestión de botnets, que infectan los dispositivos electrónicos, son algunos de los ejemplos más comunes y cada vez mayores de empresas criminales que desafían la ley penal y la administración de la justicia en la actualidad. Parece que las actividades más criminales en estos días son de carácter organizado. Con los grandes avances en el hardware y los principales avances en el software, también es más fácil de manipular el sistema. Las capacidades sofisticadas, avanzadas, casi de pertenencia a un culto, necesarias para ser un hacker hace pocos años no se necesitan mucho más. Casi todo el mundo, se dice, puede ser un hacker o participar en actividades fraudulentas a través del Internet. En muchos países en desarrollo, se ha informado, esto está bajo el control de grupos de jóvenes que participan en el fraude y la estafa.

En todo el mundo, los delitos cibernéticos cubren todo el espectro de posibles actividades criminales, de delitos financieros a los ataques destinados a comprometer la confidencialidad, integridad y accesibilidad del sistema. La percepción de la cantidad y peligrosidad de los delitos informáticos varían. A menudo hay una gran diferencia entre la conciencia, la percepción y el reconocimiento por parte del sector privado en comparación con los de las entidades gubernamentales. Por diferentes razones, que van desde la falta de reconocimiento de los delitos cibernéticos en la ley o ninguna formación para la policía para reconocer y perseguir estos delitos, las estadísticas oficiales son especialmente poco fiables o al menos muy limitadas. Las encuestas de victimización, donde se han llevado a cabo, parecen dar resultados más correctos como lo hacen para otros delitos, así, normalmente.

Las leyes sobre delitos informáticos

* Le présent rapport général est basé sur les rapports nationaux fournis par les 18 sections nationales. Les rapports nationaux sont résumés plus en détail dans le Résumé des Rapports Nationaux. Ce document suit le format du questionnaire de la section II.

Como para cualquier otro problema social y penal, la ley es el instrumento de elección en el tratamiento de la ciberdelincuencia. No hay duda de que, más que en otras áreas, se necesita una fuerte cooperación, coordinación, y normas al nivel internacional. Sin embargo, esto no siempre se pone en práctica pues que las leyes reflejan diferentes intereses, culturas jurídicas, comprensión de los derechos humanos, especialmente de la libertad de expresión y de la privacidad, y también diferentes intereses y posiciones relativas de poder. Varios aspectos deben ser cubiertos por las leyes, en primer lugar definir y declarar determinadas conductas como delitos cibernéticos. Entonces hay muchas otras áreas de intervención necesaria como cuestiones de procedimiento, los problemas de competencia, retos para la colaboración internacional y la, a menudo controvertida, responsabilidad penal y / o civil de los "ISP", los proveedores de servicios de Internet. Dieciocho países respondieron al cuestionario de encuesta de la sección II, la gran mayoría de ellos de Europa; dos, Brasil y Argentina, de América del Sur; uno, los Estados Unidos, de América del Norte; uno, Japón, de Asia; ninguno de África o de Oceanía. Por lo tanto, los resultados deben ser puestos en este contexto, y son algo limitados. Sin embargo, esto también puede reflejar el estado de la ley internacional. No muchos países tienen leyes sustantivas y procesales adecuadas en materia de ciberdelincuencia. En realidad, hay una situación desigual con Europa y América del Norte, sobre todo, que tienen una legislación muy desarrollada, mientras que muchos otros países todavía no tienen un cuerpo real de ley en este ámbito. Por lo tanto, existe un desequilibrio entre las diferentes regiones del mundo. Generalmente y más fácilmente países adoptan una legislación penal que proscribe ciertos delitos cibernéticos. No muy a menudo esto es acompañado por la ley procesal necesaria para abordar áreas difíciles como la prueba electrónica, protocolos de investigación, las cuestiones de jurisdicción especial que va más allá de las fronteras y los acuerdos que regulan la asistencia y la cooperación internacionales. Esto es definitivamente un área legal " en construcción".

I. Prácticas Legislativas y conceptos jurídicos

1. Derecho Internacional y la Codificación de las Leyes Penales

El Convenio sobre la Ciberdelincuencia, también conocido como la Convención de Budapest, es el primero y sigue siendo el único tratado internacional que intenta abordar crímenes del ordenador, Internet y electrónicos. Se trata sobre todo de armonizar las leyes nacionales; innovar y reforzar las técnicas de investigación; y fomentar la colaboración entre diferentes naciones, al principio en su mayoría europeas. Adoptada por el Comité de Ministros del Consejo de Europa el 8 de noviembre de 2001, entró en vigor de forma relativamente rápida, en menos de tres años, el 1 de julio de 2004. A partir de mediados del 2013, 39 Estados la han ratificada, la mayoría en Europa, sino que incluye cuatro países no europeos como, por ejemplo, Estados Unidos (2008). Canadá y Japón, mientras que participaron activamente en la redacción de la Convención, aún no la han ratificada. El objetivo principal de este Convenio es establecer un marco jurídico y una política criminal común contra el delito cibernético definido principalmente como la infracción de derechos de autor, las actividades fraudulentas que utilizan el Internet, la pornografía infantil, los delitos de odio y los ataques contra la seguridad de la red. Hay retos considerables en la aplicación de la Convención debido a las tradiciones jurídicas y valores constitucionales diferentes, como, por ejemplo, la protección más fuerte de la libertad de expresión en los Estados Unidos, que limita la aplicación de algunas prohibiciones de pornografía infantil, los delitos de odio, la xenofobia y las disposiciones de la Convención y de su Protocolo adicional de 2008 contra la difusión de material racista y xenófobo a través de medios electrónicos. La última década ha sido testigo de una creciente actividad en la elaboración, discusión y en ocasiones la adopción de instrumentos regionales e internacionales con el objetivo de combatir el delito cibernético. Algunos de ellos son obligatorios, mientras que otros no lo son. Entre las organizaciones internacionales activas en el campo, además del Consejo de Europa, son la Unión Europea, la Liga de los Estados Árabes, las Naciones Unidas, la Comunidad de Estados Independientes (CEI), la Comunidad Económica de los Estados de la África Occidental (CEDEAO), la Organización de los Estados Americanos (OEA) y las Naciones Unidas. La mayoría de los países que respondieron al cuestionario de la Sección II mencionó el Consejo de Europa y la Unión Europea como las fuentes más importantes de sus leyes sobre el cibercrimen, y también como el fundamento de su legitimidad y autoridad en la introducción de tales leyes. Es importante tener en cuenta el elemento transnacional de muchos tipos de delitos cibernéticos. La actividad criminal puede ser originaria de fuera del país, a veces a propósito para salir de los problemas jurisdiccionales.

2. Leyes nacionales y decisiones judiciales

Los países en general enfrentan al problema de la delincuencia informática con mayor frecuencia a través de su derecho penal, penalizando los diversos aspectos de la misma. Es el derecho penal tradicional que proporciona las definiciones y sanciones necesarias, a veces complementado por leyes especiales. Por lo tanto, las categorías generales existentes de los crímenes son a menudo tomados y utilizados para hacer frente a la novedad de la ciberdelincuencia.

Todos los países se centran en primer lugar en la creación de una tipología especial de los aspectos centrales de la delincuencia cibernética. La única excepción es Brasil, donde al parecer no hay ninguna referencia a los delitos cibernéticos en el código penal. En Alemania también existe un código especial sobre los delitos informáticos, pero muchos delitos informáticos se encuentran en el código penal. Al igual que en el caso de muchos otros países, no existe un enfoque sistemático. En los Estados Unidos hay una gran variedad de códigos y títulos desde 1970 que penalizan el robo de las computadoras, los ataques directos contra los ordenadores, y la conducta criminal que usan computadoras. En general, el impacto de las decisiones judiciales es limitado. Varios países informan poca jurisprudencia hasta la fecha. Por ejemplo, las sentencias judiciales en Alemania tienen un impacto limitado en la legislatura. Muy pocas decisiones judiciales han dado lugar a la modificación de la ley sobre el delito cibernético. Las únicas excepciones son Rusia, Estados Unidos y Japón. En Rusia, según informes, la Corte Suprema de Justicia desempeña un papel activo en la aplicación de las disposiciones específicas de fraude informático, mientras que en los Estados Unidos, como se espera de un país de derecho común, las decisiones judiciales tienen un profundo impacto en el derecho penal relativo a los delitos cibernéticos. En Japón, mientras que los legisladores no fueron muy activos en la promulgación de nuevas leyes penales o enmendar las leyes existentes, el poder judicial juega un papel fundamental a través de la interpretación extensiva de la ley penal ya en 1987.

Cada vez más, los países ahora también se mueven a otras áreas relacionadas como la investigación de los delitos cibernéticos; cuestiones de competencia que son especialmente complejas debido a la naturaleza internacional de la delincuencia electrónica; el campo en proliferación de pruebas electrónicas y la creciente necesidad de asistencia y cooperación internacional.

II. Delitos cibernéticos específicos

4. Intencionalidad

En lo que respecta al estado deseado de la mente, la categoría fundamental es la intención o la falta de ella. Al igual que en las categorías de delitos, el estado mental del autor del delito es de gran importancia. En todos los países que presentaron informes, se requiere la intencionalidad general. Por supuesto, es esencial tener en cuenta las diferentes definiciones o interpretaciones de la "intención". Brasil requiere intención específica cuando se trata de obtener, alterar o destruir datos o hacer que el sistema sea vulnerable a fin de obtener una ventaja ilícita. En Japón también se requiere una intención específica de muchos delitos en forma de "a los efectos de".

5. Negligencia

Más allá de las señales básicas de intención general, intención específica o la falta del mismo, diferentes tradiciones jurídicas impactan el lenguaje usado aquí. Diferentes tonalidades de los conceptos básicos de la negligencia pueden aparecer bajo sellos como " a propósito "," conocimiento "," negligencia "e" imprudente". En general, la mayoría de los países informan de que hay actos de negligencia en el campo, pero sorprendentemente en 6 no existen. En general, muy pocos delitos pueden ser cometidos por negligencia.

1. Integridad y funcionalidad del sistema de Tecnología de la Información

A. El acceso ilegal y la interceptación de la transmisión

El acceso a un sistema informático es el primer paso necesario para operaciones posteriores y por lo tanto muy esencial. Por lo tanto, un intento de ganar el ingreso no autorizado a un sistema informático es una de las primeras actividades ilegales llevadas a cabo y más generalmente penalizado. En un proceso continuo que puede ir de una entrada ilegal en un sistema con el objetivo de sólo mirar alrededor y ver lo que hay que pueda ser de interés al robo de información y del contenido para su propio beneficio, hasta hacer que el contenido sea inaccesible. El principal efecto negativo es comprometer el acceso, la integridad y la funcionalidad del sistema. Se abre la puerta al robo de identidad, a las actividades fraudulentas y falsificaciones y, finalmente, a las acciones más complejas, insidiosa y dañinas a través de la implantación de virus, malware y botnets. No es de extrañar que todos los países que respondieron a la encuesta AIDP lo penalicen. Algunos utilizan la expresión con el calificador específico: " el acceso sin autorización». Para algunos, como los EE.UU., sencillamente el acceso, sin o excediendo autorización, es suficiente para

constituir un delito. No es necesario el uso de un software especial para derrotar el sistema y sin autorización o superior es suficiente para constituir un delito. No es necesario el uso de un software especial para derrotar el sistema. La excepción es Brasil, que tiene una prohibición específica de acceso ilegal. Para muchos países, la producción, oferta, distribución, venta y / o posesión de software o dispositivos de piratería es un delito autónomo.

Por lo tanto, las leyes de los países que respondieron al cuestionario AIDP Sección II aplican diversos tratados y acuerdos internacionales o regionales contra la delincuencia cibernética. Uniformemente, prohíben el acceso ilegal a un sistema electrónico. Se debe tener en cuenta que algunos países se centran más en los datos o la información almacenada en un sistema que en el propio sistema. Otros, como Rusia, no protegen a toda la información. Ellos exigen que la información ya esté protegida por la ley. Para complicar las cosas algunos países, como Turquía, Polonia, Italia, Suecia, Brasil, Bélgica y Luxemburgo no definen específicamente uno o más elementos como el equipo o los datos electrónicos. Algunos países consideran que la entrada sin autorización es suficiente para que el crimen tenga lugar mientras que otros requieren un elemento adicional como la intención o una acción que sigue a la entrada no autorizada. Para algunos, la entrada ilegal es un delito sólo si está relacionado con el comportamiento delictivo grave posterior. Parece que aquí hay diferencias importantes con algunos países que consideran suficiente el mero acceso sin autorización, mientras que otros requieren más elementos, relacionados, por ejemplo, a la intención o a las consecuencias de la entrada ilegal como copiar la información, cambiarla, o perturbar el funcionamiento del sistema, de la red, etc. Por lo tanto hay una zona gris aquí sobre la suficiencia de la mera entrada frente a la necesidad de acciones adicionales. También la naturaleza del delito o los delitos cometidos juega un papel con algunos países que sólo penalizan la entrada si se conecta a ulteriores delitos graves. Como se puede esperar, cuyo equipo es y cuál es el valor de la información o de los datos almacenados en él también juegan un papel importante en la determinación de si se trata de un crimen o no o la gravedad del mismo. También hay circunstancias agravantes, como la distribución, divulgación, venta, publicación, etc. de los datos o informaciones así obtenidas. En el caso de importantes datos de inteligencia y de seguridad gubernamentales, esto puede dar lugar a graves acusaciones de traición y / o ayudar al enemigo.

B. Los datos y la interferencia del sistema

Muy relacionado con las actividades ilegales previas, la interferencia con el sistema y con los datos está penalizada en muchos países. Intercepción no autorizada, destruir, borrar, dañar, alterar la información y datos importantes u obstruir el acceso es un crimen para la mayoría de los países que respondieron al cuestionario de la AIDP. La interceptación se extiende a la protección de los datos que se transmiten, además y más allá de los que están siendo almacenados. Esto pone de relieve la confidencialidad y privacidad de los datos en tránsito. En este caso, puede haber diferencias sustanciales. Por ejemplo, los tribunales estadounidenses no han ampliado la protección de la privacidad del correo en tránsito a los datos electrónicos que se transmiten.

C. Falsificación de datos

Con pocas excepciones, la mayoría de los países reconocen como delito producir datos falsos o falsificar datos auténticos. Con el fin de proteger los intereses financieros de todo, se criminaliza el uso fraudulento de procesamiento de datos. Los operadores y todas las personas que participen en general son sancionados. Algunos países, como Finlandia y Suecia, no tienen leyes especiales sobre la falsificación de datos. Utilizan disposiciones generales en lugar de falsificación. En los EE.UU., algunos estados, como Georgia, tienen estatutos específicos de falsificación. Un reto importante es que algunos países, como por ejemplo Alemania, no tienen una definición legal del ordenador y / o de los datos electrónicos. Algunos investigadores proponen que los datos deben significar "una descripción electrónica de la información". Desde que incluyan los datos, la definición abarca programas de software también.

D. El mal uso de los dispositivos y la piratería

Software, dispositivos, contraseñas y códigos utilizados para acceder sin autorización o derecho sistemas electrónicos están muy en demanda y en uso hoy en día, y no sólo por individuos u organizaciones privadas. La aplicación de la ley penal al mal uso de los dispositivos y la piratería es complejo, debido a las distintas etapas, el requisito de la intención o al menos el conocimiento, la conciencia del por qué, de la razón por la cual estos elementos pueden obtenerse o ser utilizado, así como la importancia de distinguir entre los diferentes tipos de hackers: los hackers "sombrero blanco" o "éticos" que ponen sus habilidades hacia la identificación de debilidades sistémicas que permitan la entrada ilegal, con el objetivo de exponer la

vulnerabilidad y su corrección frente a los hackers "sombrero negro" o "non éticos" que intentan el ingreso no autorizado y realizar actividades ilegales. La protección de los hackers "sombrero blanco" de la persecución para que puedan realizar su servicio valioso es perseguido en algunos países. En los Estados Unidos, según los informes, la Administración Nacional de Seguridad ofrece la certificación de hackers "éticos" y este tipo de piratería ha sido ampliamente utilizado por los militares. En general, la mayoría de los países penalizan software, dispositivos, contraseñas y códigos que permiten o facilitan el acceso no autorizado o ilegal a los sistemas electrónicos. Sin embargo, hay matices sutiles. Por ejemplo, Argentina no penaliza el desarrollo de herramientas, aplicaciones y programa. Dinamarca no penaliza herramientas de un hacker. El uso no autorizado de la caja de herramientas de un hacker no está tipificado como delito en Austria. En Italia, Rusia y Suecia no se penaliza la simple posesión de un herramientas de hackers; se requiere más información sobre la intención, objetivo, "a sabiendas ", etc. Rusia tipifica software sólo si es deliberadamente diseñado para la piratería y, además, el autor debe tener la intención de utilizar estas herramientas para cometer delitos. Aunque Japón no penaliza el intento de acceso no autorizado, criminaliza explícitamente el "uso " de un registro electromagnético que da un comando no autorizado para la ejecución en un ordenador de otra persona sin motivos justificados. Los Estados Unidos, como Rusia, requieren que una persona sabe o tiene razones para saber que el propósito de un dispositivo es la piratería. También en Alemania el delito requiere que el objetivo del actor criminal es de causar daño a la persona que está autorizada a usar los datos. Un enfoque diferente es tomado por el Reino Unido. Si bien no hay ningún informe de ese país, vale la pena señalar que el acceso no autorizado, incluso de "sombrero blanco" para exponer las vulnerabilidades para el beneficio de muchos, no es legal allí. El Código Penal alemán castiga actos preparatorios de un delito, pero, en forma incongruente, no penaliza la tentativa de cometer el mismo delito. Dado que la mayoría de los intentos deben incluir un poco de preparación, esta falta de lógica es atenuada. La producción, la adquisición, la venta, el suministro, la difusión o proporcionar una contraseña u otros códigos de seguridad que permiten el acceso a los datos se consideran como delito. También se penaliza a los mismos hechos relacionados con el software. No hay ninguna disposición que exime actividades de hacking de "sombrero blanco" de ser consideradas un delito. El único elemento que puede ayudar a excluir la responsabilidad penal es la ausencia de mens rea. No hay ninguna pena para la distribución de información hacheada en general. Sin embargo, la divulgación de secretos comerciales o industriales para el público se castiga como la distribución realizada con la intención de obtener ganancias financieras o causar daños financieros a los demás. La mera posesión de una herramienta de hacker no está tipificada como delito específico en el Código Penal alemán. Se considera una infracción administrativa.

Kits de herramientas de hacker no están estrictamente regulados en los EE.UU. Es penalizado su uso sólo si la información o los datos resultantes son divulgados. El foco en los EE.UU. es el desarrollo de contramedidas fuertes, aumento de la conciencia pública, y la transferencia de la responsabilidad al usuario que debe tener antivirus, protección anti-malware, etc., su actualización periódica, en lugar de centrarse en la piratería, sobre todo también para proteger a los piratas informáticos, gubernamentales y militares "éticos".

2. Intimidad

A. Violación del secreto de los datos privados

Los datos privados se definen como los datos que pertenecen a la vida privada de las personas, pero non identifican o hacen posible identificar a una persona, por ejemplo, estado civil, orientación sexual, estado de salud, hábitos o preferencias de compra. Estos datos son a veces recogidos automáticamente, puesto que ya existen en la cuenta electrónica de la persona, por ejemplo a través de cookies o que se obtienen de las personas que deben proporcionar esta información con el fin de obtener ciertos beneficios como el seguro médico, tarjeta de crédito, una cuenta bancaria, licencia de conducir, el registro de un programa o un curso en una universidad, obtener una membrecía en una organización, club, viajeros frecuentes o programa de cliente frecuente, etc. Teniendo en cuenta las muchas revelaciones, especialmente por Wikileaks, Edward Snowden y otros, el tema de lo que la "privacidad " en realidad significa hoy en día, el valor real de las promesas de proteger dicha privacidad de los recolectores de datos en comparación con las prácticas actuales, y el papel de los distintos organismos gubernamentales que legalmente, ilegalmente, bordeando la ley o la interpretación de la ley para su beneficio puede jugar, es de suma importancia. Se ha informado, por ejemplo, que, aunque Microsoft promete a sus usuarios de respetar su privacidad, colaboró estrechamente con los servicios de inteligencia de Estados Unidos para permitir las comunicaciones de los usuarios a ser interceptadas, incluyendo ayudar la Agencia de Seguridad Nacional para eludir su propia encriptación de mensajes y chats de la empresa. Según se informa, este es sólo un ejemplo de esta colaboración por parte

de muchos proveedores de servicios por Internet. En junio de 2013, el periódico The Guardian reveló que la Agencia de Seguridad Nacional afirmó tener "acceso directo" a través del programa Prisma a los sistemas de muchas compañías de Internet más importantes, incluyendo Microsoft, Skype, Apple, Google, Facebook y Yahoo. También se ha informado en los medios de comunicación que, si bien la Unión Europea y varios países europeos expresaron su indignación por haber sido espiado por los EE.UU., que en realidad cooperaron e incluso participaron en el programa en diferentes medidas. También ha salido a la luz que hay una creciente vinculación e intercambio de información entre los programas de espionaje de los organismos militares y de seguridad y vigilancia de EE.UU. y el sector privado, especialmente con las empresas financieras y bancarias, dando a las elites información valiosa e incluso avanzar para continuar a dominar los mercados. Todo esto debe ser tenido en cuenta, al menos, para poner en perspectiva las diversas afirmaciones, garantías y leyes que supuestamente rigen y protegen la privacidad de los ciudadanos y los consumidores en varios países. Si bien las leyes pueden de hecho tener un efecto protector de la privacidad como se escriben, es su aplicación y su observancia que se pone en duda por el cada vez más poderoso sistema de aprovechamiento global del sistema electrónico en todo el mundo de las comunicaciones por el poder político, militar y económico e incluso la hegemonía, con la estrecha colaboración del sector privado. Según varios informes de prensa, el reglamento y directiva de la Unión Europea propuestos para proteger la privacidad de los ciudadanos y de los consumidores se están debilitando y se pospusieron debido en parte a la presión quieta pero intensa de los Estados Unidos y de los principales proveedores de servicios de Internet. La minería de datos es demasiado rentable. Los fundamentos jurídicos, éticos y cívicos de la privacidad prometido al ciudadano y al consumidor por la ley, cuando exista, y por los gigantes de los medios electrónicos y sociales tienen que ser modificados, reconstruidos y reforzados a nivel internacional para tener un mínimo de credibilidad y eficacia.

Todos los países que respondieron al cuestionario AIDP para la Sección II tienen, en distinto grado, elaborados sistemas de ley que supuestamente protegen los derechos de los ciudadanos y de los consumidores cuando utilizan el sistema electrónico para acceso a las redes sociales; inscripción para diversas actividades, programas y membrecías; la realización de transacciones financieras y bancarias; la obtención de diversos tipos de seguro médico; y llevar a cabo cada vez más sus vidas a través de instrumentos y sistemas electrónicos. Los recolectores de datos, por lo general, están obligados a revelar sus prácticas de información antes de recolectar información privada de los consumidores, informar al consumidor de la identidad corporativa para la cual está recogiendo las informaciones, y esbozar las medidas adoptadas por el recolector de datos para garantizar la confidencialidad, la integridad y la calidad de los datos. La mayoría de los países también requieren que se publique la política de privacidad. No revelar la política de privacidad se trata en algunos casos como un delito menor (Croacia) y en otros casos como una infracción administrativa (Italia) castigado con una multa (Dinamarca). Cabe señalar que en los Países Bajos los datos no se consideran bienes, por lo que no están sujetos a los delitos de propiedad. La Ley de Japón sobre la Protección de Datos Personales no penaliza la transmisión y la distribución de los datos privados como tal, a menos que estén clasificados como "secretos comerciales". La Ley Federal Alemana de Protección de Datos acertadamente requiere que los datos personales deben ser recogidos con la ayuda de la persona que tiene los datos, la persona interesada. Esto requiere el conocimiento y el consentimiento del titular de los datos, así como su participación en el proceso de recogida de los datos. Esto se hace para asegurarse de que él u ella puede decidir sobre la divulgación de los datos personales que se recopilen. El derecho de recoger datos sobre una persona sin que esa persona lo sepa, se da sólo en circunstancias excepcionales. Si los datos son recogidos sin el consentimiento del titular de los datos, las obligaciones especiales de información deben cumplirse después. La notificación deberá ser generalmente comprensible. Cabe señalar que el incumplimiento de estas obligaciones no conduce ni a sanciones penales ni administrativas. El interesado debe solicitar la reparación en el sistema de derecho civil. También hay ninguna disposición básica que penaliza en general la transferencia y la distribución ilegales de los datos privados. Cabe señalar que en la legislación alemana, la recopilación de datos, procesamiento y uso puede ser legal si la ley lo permite a través de diversas leyes específicas o si existe el consentimiento del interesado. Estos principios jurídicos son aplicables a las telecomunicaciones también. La recolección de datos debe ser gobernada y se justifica con los principios de necesidad, la evitación de datos, economía de los datos, y el propósito. En los EE.UU. no hay una ley integral. Hay leyes especiales como la Ley para la Privacidad de los Niños en Línea; la Ley Gramm- Leach- Billey que requiere que las instituciones financieras establezcan las garantías adecuadas y proporcionen una indicación clara y visible a los consumidores; y la Ley de Portabilidad del Seguro de Salud que regula el uso y la divulgación de información de salud

protegida. Existe una gran preocupación por la protección de la privacidad de la base de datos creada por la Ley de Portabilidad del Seguro de Salud (la llamada "Obamacare"), que cubrirá toda persona en los EE.UU. Esta enorme base de datos incluirá los datos de ingresos y financieros, tamaño de la familia, la ciudadanía y el estatus migratorio, estado de encarcelamiento, número de seguro social e información privada de salud. Se compilarán los archivos de todo el mundo en los Estados Unidos y se obtendrá la información del Servicio de Rentas Internas (IRS), el Departamento de Seguridad Nacional, el Departamento de Defensa, la Administración de Veteranos, la Oficina de Administración de Personal, la Administración del Seguro Social, el Cuerpo de Paz, y bases de datos estatales de Medicaid. Por ejemplo, el ingreso anual reportado se comparará con las declaraciones de impuestos y puede ser corregido en consecuencia, si hay una discrepancia. En primer lugar, existe la preocupación de que esta base de datos será un blanco irresistible para los hackers. Además, la ley prevé que los grupos comunitarios y sin fines de lucro centrados en el consumidor, llamados " Navegantes ", podrá acceder a la información con el fin de recibir fondos de los intercambios de la salud para que puedan educar al público sobre el nuevo sistema de salud obligatorio y también proporcionar adecuada referencias a los proveedores de seguros. El potencial de abuso es muy alto. El potencial de ganancia en la venta de una información tan detallada y oficial para todo tipo de propósitos, como el empleo, la carrera, el nivel de ingresos y el poder adquisitivo, los seguros, las inversiones, la empleabilidad, la admisión a ciertas líneas de trabajo o la carrera profesional, la historia clínica y la comercialización de remedios, medicamentos, incluso idoneidad para el matrimonio en algunas culturas étnicas, etc., va a ser muy fuerte. Con tantas organizaciones privadas que tienen acceso a tal información valiosa sobre prácticamente cada persona de los EE.UU., algunos delitos informáticos y expertos en privacidad esperan mayores incumplimientos y violaciones.

En los Estados Unidos, mientras que hay una necesidad de publicar las políticas de privacidad, no hay sanciones penales en caso de no hacerlo.

B. Violación del secreto profesional

En la mayoría de países que presentaron informes, el Código de Procedimiento Penal garantiza la confidencialidad de los abogados, clérigos, médicos, psicólogos, psiquiatras y otros. Información personal y / o familiar adquirida por los profesionales como parte de su ocupación está protegida. Sin embargo, hay límites. Normalmente existe la obligación de informar si el secreto revelado es en el interés público o el interés predominante de un tercero (por ejemplo, el abuso infantil), si hay un delito grave que se está cometiendo o si se amenaza de cometerlo, y si una persona inocente está en riesgo de ser acusada o condenada por un delito. Sin embargo, por ejemplo, no hay ningún requisito general de la legislación finlandesa para reportar un crimen; pero, si el delito todavía se podría evitar, puede haber responsabilidad penal por el hecho de no informar de ello.

Por otro lado, la ley italiana exige que los profesionales den a conocer su colección de información y sus prácticas de gestión de la misma antes de recoger información personal de los pacientes o clientes. Ellos tienen que revelar sus prácticas de procesamiento de datos, pero no sus obligaciones éticas. Tienen que informar al paciente o cliente de su control sobre la divulgación de los datos personales. La ley prevé una protección especial para los datos de identificación, sensibles y judiciales.

En Alemania, la Ley Federal de Protección de Datos protege los datos personales. Obligaciones específicas de secreto profesional se aplican, por ejemplo, a los miembros de los organismos de servicio público sobre la información que obtengan en el ejercicio de sus funciones profesionales. Lo mismo sucede con el personal médico, abogados y asesores fiscales. Sin embargo, la revelación de secretos autorizadas por la ley es legal. El consentimiento del sujeto del secreto u otra justificación como necesidad (pe carboncillo prevenir un peligro inminente) también hace que sea lícito revelar secretos. El interés público también puede ser considerado de mayor valor que el interés de la persona en la protección de la confidencialidad de la información. Por lo tanto, los profesionales médicos deben revelar ciertas enfermedades cuando las agencias de salud pública así lo requieran; las enfermedades ocupacionales a las compañías de seguro; los fármacos prescritos que sustituyen a las drogas ilegales; informar a las compañías de seguros de salud y notificar a las autoridades de los nacimientos o muertes. Todo el mundo debe revelar información sobre los delitos graves previstos. El Código Penal alemán lista en detalle aquellos profesionales que tienen el deber de mantener en secreto la información confiada a ellos. La divulgación y la explotación de secretos personales son criminalizados.

En cuanto al mundo de los negocios, en los Países Bajos es un crimen hacer pública intencionalmente la información que uno está obligado a mantener en secreto, como, por ejemplo, en relación a la empresa donde uno trabaja.

C. Procesamiento ilegal de datos personales y privados

En los Estados Unidos, el uso ilegal, la transferencia y distribución de los datos privados no está tipificada como delito. Si alguien sufre un daño, deben buscar una reparación de naturaleza civil, lo que puede implicar una realización costosa. En otros países (por ejemplo, Brasil) la transferencia ilegal y distribución de datos privados no se incluye específicamente en la ley. Con otras palabras, en Croacia, Dinamarca, Finlandia, Italia, Turquía, el uso ilegal, la transferencia y la distribución de los datos privados es criminalizada. En Alemania, la recolección ilegal, la retención y transferencia de datos personales son criminalizados. Sin embargo, el uso ilegal en general no se criminaliza, sino que depende de la situación y el contexto. La recolección de datos por las autoridades policiales en Alemania es legal sólo si las disposiciones legales especiales permiten. En Japón, mientras que la adquisición ilegal de los datos personales y la información constituye un delito, una conducta no autorizada en relación a los datos privados no ha sido muy penalizada, con la excepción de los secretos comerciales. El robo de datos personales no representa un problema legal grave en Rusia como en los EE.UU. o Europa. La primera ley fue aprobada en 2006, después de la ratificación del Convenio del Consejo de Europa para la protección de las personas y prevé la responsabilidad penal. Sin embargo, no existen disposiciones especiales para las infracciones que se cometen en la red informática. El enfoque de esta cuestión en los Países Bajos es muy interesante. Los datos no se consideran "bienes" en el derecho penal holandés. La razón es que la falta "singularidad." En realidad, son múltiplos. Una persona que controla los datos no pierde necesariamente el control de ellos si otra persona obtiene acceso a ellos, por ejemplo, copiándolos. Él o ella todavía tiene. Así, los delincuentes que envían información robada a terceros digitalmente no son punibles a menos que también sean el hacker.

E. Robo de Identidad

La gran cantidad de posibilidades para las comunicaciones personales, la publicación de los datos personales, las fotografías, y aún más la automatización de procesamiento de datos y el crecimiento exponencial de todos los tipos de transacciones que no son nada más cara a cara también han incrementado las oportunidades para la robo de información personal que afecta a la identidad de uno, especialmente la financiera, a través del uso de sistemas electrónicos. Objetivos favoritos son la información sobre tarjetas de crédito, cuentas bancarias, documentos de identificación, como licencia de conducir o el pasaporte, y las direcciones IP. Esto se puede hacer a través del acceso no autorizado a los dispositivos electrónicos de alguien y / o las cuentas que fueron discutidas previamente como paso fundamental para la comisión de los delitos cibernéticos, mediante malware, phishing o la obtención ilegal de información en virtud de su posición, contactos, o el acceso de uno a bancos de datos. Revelaciones de hackers que obtienen acceso y roban miles de millones de registros de tarjetas de crédito de usuarios que se venden o utilizan para el chantaje y la extorsión son bastante frecuentes. Por otra parte, la divulgación no autorizada de la vigilancia penetrante, generalizada y omnipresente del gobierno, de la interceptación, y de programas de espionaje contra ciudadanos y extranjeros por igual, almacenados en bancos de datos masivos, se han sumado a la percepción y el conocimiento de la fácil disponibilidad de información de todo tipo sobre millones de personas. Estos datos son accesibles a voluntad y no se tiene siempre que demostrar una "necesidad de conocer " por los empleados de los contratistas gubernamentales, cuya ética y capacidad de resistir a las tentaciones adecuadas no siempre son sus rasgos más fuertes. La obtención, transferencia, uso de los datos personales así obtenidos por actividades criminales sin duda debe ser criminalizados. En realidad, a nivel internacional, parece que no existe un instrumento internacional vinculante que anticipa y prohíbe el robo de identidad. A nivel nacional, sobre la base de las respuestas al cuestionario AIDP Sección II, la mayoría de los países utilizan las disposiciones generales para criminalizarlo; algunos utilizan disposiciones específicas, y otros no lo prohíben como delito. Por ejemplo, Argentina, Austria, Brasil, Croacia, Dinamarca, Finlandia, Alemania, Italia, los Países Bajos, la Federación de Rusia y Suecia no tienen en su Código Penal una prohibición específica de robo de identidad. Sin embargo, en Alemania, por ejemplo, las acciones específicas sobre el robo de identidad pueden ser criminalizadas como infracciones administrativas o penales. Con más detalle, Brasil incluye el robo de identidad en los delitos contra la propiedad; en Croacia puede ser prohibido como uso ilícito de los datos personales; en Dinamarca bajo leyes contra la falsificación, el robo y el fraude; en Italia se pueden aplicar otras categorías como la suplantación, la ganancia o daño financiero o engañar a la víctima; y en los Países Bajos se puede usar el

delito de fraude o extorsión. La posición de Finlandia es bastante interesante ya que no clasifica a la identidad de una persona como un bien mobiliario que puede ser robado. Los pocos países restantes, Bélgica y Luxemburgo, Polonia, Rumania, Turquía y los Estados Unidos cuentan con disposiciones específicas. En Japón, el phishing se ha sancionado recientemente; sin embargo, no existe una disposición penal que castiga los ataques a la personalidad digital de una persona.

3. Protección contra los contenidos ilícitos

A. Objeto

i. Pornografía Infantil

El importante papel de Internet en la difusión mundial de la pornografía es bien conocido. La disponibilidad inmediata de material pornográfico en la privacidad total de la residencia o espacio personal de uno fue un poderoso incentivo para que un gran número de personas se juntase a la Internet. Hay quienes sostienen que, en gran parte, sobre todo al principio del fenómeno de Internet, era la pornografía que impulsó la expansión meteórica de Internet y ha demostrado su utilidad potencial de hacer. El anonimato y la privacidad fueron factores muy atractivos. Esto más aún cuando se trata de acceder a la pornografía infantil, con su connotación penal y su apunta a la perversión sexual del usuario. Especialmente en tiempos más recientes, se ha producido un gran esfuerzo internacional para intervenir eficazmente contra la pornografía infantil a disminuir en gran medida, y con suerte eliminar, la facilidad de la difusión de las imágenes y la rentabilidad de la misma. Desalentar la circulación de esas imágenes será en el fin proteger a los niños e interrumpir, de forma óptima eliminar, el mercado de este material.

Todos los países que respondieron al cuestionario penalicen producir, transmitir, proporcionar, transportar, exportar, acceder, descargar y almacenar imágenes de pornografía infantil. También prohíben el uso de medios electrónicos en todas las funciones relacionadas con la producción, distribución, acceso, descarga, posesión y exportación de pornografía infantil. En Japón estas actividades a través de Internet se incluyeron en 2004, con la modifica de la Ley sobre la represión de actividades relacionadas con la prostitución y la pornografía infantiles. En 2009 Alemania aprobó una ley que requiere los proveedores de Internet de bloquear sitios web que muestran material pornográfico infantil. Sin embargo, la ley no se aplicó y finalmente fue derogada en el 2011. En la actualidad, los proveedores de servicios de Internet (ISP) directamente borran la pornografía infantil en Alemania, en cooperación con la Agencia Federal de Policía. La Asociación Internacional de Líneas Directas de Internet (INHOPE) desempeña un papel activo en todo esto, en cooperación con las autoridades nacionales. Si un contenido pornográfico infantil es detectado por uno de los miembros de la red, se establece un contacto con los socios nacionales de INHOPE. Se solicita al proveedor de almacenamiento, que es responsable de la transmisión de los contenidos, que lo elimine. En Europa, negarse a eliminar el contenido ilegal es un delito penal. Por lo tanto, los esfuerzos para erradicar la pornografía infantil son bastante exitosos. En relación con el tráfico, en algunos países, por ejemplo, Italia, Países Bajos, también se incluye la prohibición de "grooming", atraer y explotar a los niños, y de solicitar en línea a los niños, al igual que Argentina, con fines pornográficos. Una excepción importante es la de Bélgica y Luxemburgo, donde la ley no incluye específicamente el uso de la Internet para atraer y explotar a los niños con fines sexuales. Algunos países no definen expresamente la pornografía infantil: Polonia, Rusia y Suecia. La mayoría de los otros países utilizan definiciones de acuerdo con las normas internacionales, como Argentina, Austria, Croacia, Dinamarca, Finlandia, Italia y Estados Unidos. La definición de Japón es diferente de las normas internacionales. Finlandia no utiliza el término " pornografía infantil " o "espectáculo pornográfico " en su Código Penal. Utiliza "sexualmente obsceno. " En el caso de los países que carecen de disposiciones específicas en materia de pornografía infantil, puede ser perseguible por otra legislación. En Rusia, por ejemplo, el contenido ilegal prohibido en este caso es la actividad extremista en las comunicaciones públicas que pueden dañar a los niños. Por lo tanto, se puede utilizar el código penal más la ley contra el extremismo. Polonia considera las redes mundiales de informática como un lugar público para hablar. Por lo tanto, las disposiciones del Código Penal relativo a la violación del orden público pueden ser aplicadas como la prohibición de obligar a alguien que no quiere a ver material pornográfico. Si bien no existe una definición legal de pornografía infantil en la legislación penal sueca, su significado es similar a la de los instrumentos internacionales. En general, es la representación visual y material que están prohibidos. Materiales de audio a menudo no están cubiertos. Además, dado que las acciones relacionadas con la pornografía infantil pueden ser cometidas mediante el uso de diferentes medios de comunicación y las imágenes disponibles fuera de línea, en varios países hay una preferencia por un enfoque genérico sobre "tecnología y los medios de comunicación neutral" en lugar de uno específico para computadoras. También

hay diferencias en el lenguaje utilizado para describir la población que debe ser protegida con el consiguiente impacto sobre el límite de edad que les da derecho a la protección. Varios países utilizan la expresión: "Menores ", como Argentina y Austria. La mayoría de los países utilizan "niños" como Croacia, Dinamarca, Finlandia, Italia, Rusia, Turquía y los Estados Unidos. Bélgica y Luxemburgo utilizan ambos, menores de edad y niños. Polonia en su lugar utiliza la edad real, hablando de niños de 15 años de edad o más jóvenes. Debe tenerse en cuenta que el Consejo de Europa permite reducir la edad hasta un máximo de 16 años de edad. La Convención de las Naciones Unidas sobre los Derechos del Niño define "niño" como "toda persona menor de 18 "(artículo 1). Algunos países abordan el tema de la pornografía infantil producida por menores de edad. Austria no tipifica como delito la pornografía hecha con el consentimiento del niño y para el uso de los niños. Croacia utiliza el límite " de 14 años de edad " para limitar la responsabilidad. La cuestión de la intención también muestra diferentes matices, dependiendo del país. Algunos países exigen que la persona que acceda a la pornografía infantil lo haga conscientemente. Para Argentina, es un crimen acceder a la pornografía infantil, transmitirla, exportarla, y poseerla si es "a sabiendas". Otros países que siguen el mismo enfoque son: Austria, Croacia, Dinamarca, y los Estados Unidos. Algunas jurisdicciones requieren tanto la intención de entrar en un sitio de pornografía infantil como sabiendo que esas imágenes están ahí: Bélgica, Luxemburgo y Suecia. Polonia e Italia no criminalizan simplemente acceder a la pornografía infantil. En Rusia " simple posesión " no está tipificada como delito. La posesión de pornografía infantil en Japón es un delito sólo si es para su distribución a los demás. Alemania exige la intención del autor para acceder a la pornografía infantil tanto en cuanto a la edad del niño como sobre el carácter pornográfico del material exhibido. La posesión de pornografía infantil por negligencia no es punible en el derecho penal alemán. También hay diferencias interesantes en cuanto a la intervención judicial. En algunos países, como Brasil, Italia, Japón y Polonia, los jueces son relativamente impotentes para intervenir. En otros países, los jueces tienen autoridad para suprimir el orden, la confiscación, decomiso, etc., como en Austria, Bélgica, Alemania, Luxemburgo, Dinamarca y Turquía. En los Estados Unidos, no hay ninguna disposición legal que permite a los jueces ordenar la eliminación de material de pornografía infantil, pero tienen facultades discrecionales para la configuración de los recursos.

Por último, la pornografía infantil virtual es un tema importante de debate y de acción legal. En algunos países, como Argentina, Turquía, Japón y los Estados Unidos, no es un crimen. No está penalizado en Austria, si la imagen es sólo para uso privado. Es un delito en Bélgica, Luxemburgo, Brasil, Dinamarca, Finlandia (si es genuina y realista), Italia, Países Bajos y Suecia. En Alemania, la pornografía infantil virtual entra en el ámbito del Código Penal, sin embargo, el material debe dar la impresión de actividades "reales" por "niños reales". Un enconado debate público sobre la conveniencia de legalizar la pornografía infantil virtual como medio para ofrecer una alternativa a los pedófilos se llevó a cabo a finales de 2012 y principios de 2013 en los Países Bajos. En cuanto a los Estados Unidos, en abril de 2002, la Corte Suprema de EE.UU. en *Ashcroft v Free Speech Coalition*, 535 EE.UU. 234 (2002) encontró la Ley de Prevención de la Pornografía Infantil inconstitucional. Aunque sigue siendo ilegal hacer, mostrar o poseer imágenes sexualmente explícitas de niños, la Corte encontró que no había ninguna razón de peso para prohibir la fabricación, exhibición o almacenamiento de las imágenes, que se limita a parecer niños. Dos categorías de pornografía que eran ilegales bajo la ley son ahora legales: las imágenes sexualmente explícitas de los modelos de vida que sin embargo parecen más joven que su edad real, e imágenes sexualmente explícitas de niños generadas por computadoras. Pues que no hay verdaderos menores involucrados en la producción de estas imágenes, la Corte Suprema de EE.UU. argumentó que debería considerarse protegida por la libertad de expresión. Sin embargo, la pornografía infantil virtual puede ser un delito si es obscena, es decir, si se carece de "LAPS " por sus siglas en ingles, vale a decir, ningún valor literario, artístico, político y científico.

ii. Cualquier otro objeto donde la penalización depende del uso de la Tecnología de la Información y de la Comunicación (TIC)

a. Creación y uso de un cierto anonimato:

Non criminalizado: Argentina, Bélgica, Luxemburgo, Dinamarca, Finlandia, Alemania, Italia, Japón, Suecia y Estados Unidos.

Criminalizados: Croacia

b. Cyber- bullying

Esta es una de las zonas más "calientes" para llamadas de criminalizar conductas que pueden ser descritas como la intimidación por medios electrónicos. Hay quienes afirman que los delitos del Código Penal

"existentes" como el acoso criminal, profiriendo amenazas, la intimidación, el uso no autorizado de una computadora, la extorsión, el libelo difamatorio y la pornografía infantil ya generalmente cubren la intimidación más grave y que, por lo tanto, no existe una legislación especial sea necesario.

En cambio, piden que el Código Penal sea revisado y modificado para poner al día ciertos delitos existentes para lidiar con el acoso a través de medios electrónicos, así como actualizar las facultades de investigación para la aplicación de la ley, de modo que todos los actos de intimidación cibernética perpetrados por medio de las nuevas tecnologías pueden ser investigados y enjuiciados efectivamente. Muchos códigos penales ya contienen disposiciones que prohíben el envío de mensajes falsos por carta, telegrama, teléfono, cable y radio, así como llamadas telefónicas indecentes y acoso. Tal como están redactados en la actualidad, estos delitos no pueden cubrir las situaciones de ciber-acoso cuando los mensajes se envían a través de texto o correo electrónico. Así, hay países en los que el acoso cibernético se penaliza específicamente y otros donde no lo es, a veces, con la justificación de que las leyes actuales pueden abordar la situación con algunos cambios menores.

No penalizan el bullying cibernético: Argentina, Finlandia (no sancionado directamente, sino el uso de la difamación es posible), Dinamarca (hay disposiciones específicas, otras leyes se utilizan también), Alemania, Italia, Japón, Suecia y Turquía. Debe tenerse en cuenta que el acoso cibernético puede ser incluido dentro de la comisión de delitos penales existentes, al igual que en Alemania, por ejemplo.

Criminalizan el bullying cibernético: Bélgica, Luxemburgo, Croacia, Polonia, Estados Unidos (leyes estatales)

c. Acoso Cibernético

No criminalizado: Argentina, Finlandia (no incluye disposiciones específicas; el uso de la orden de restricción es posible), Dinamarca (hay disposiciones específicas; otras leyes utilizadas), Italia, Japón, Países Bajos (sin ofensa separada), Suecia y Turquía. En algunos de estos países, como en Japón, por ejemplo, otras disposiciones del Código Penal se pueden utilizar para procesar al acoso cibernético.

Criminalizado: Bélgica, Croacia, Alemania, Luxemburgo, Polonia, Estados Unidos (leyes federales y estatales)

d. Cyber grooming

El grooming («acicalar») se refiere a una serie de conductas y acciones deliberadamente emprendidas por un adulto con el fin de obtener la confianza y la amistad de un menor de edad, estableciendo un lazo emocional con el mismo, con el objetivo de reducir las inhibiciones del niño y poder aprovechar sexualmente de él. En algunos casos, el objetivo podría ser la introducción del menor a la prostitución o participar en la producción de material pornográfico.

No criminalizado: Argentina, Turquía, Japón y Suecia

Criminalizado: Alemania, Italia, Países Bajos, Polonia, Estados Unidos (ley federal)

4. Violaciones de la propiedad, incluyendo la propiedad intelectual, relacionadas a la tecnología de la información y de comunicaciones

La propiedad, los activos financieros y la autenticidad de los documentos son los principales intereses protegidos aquí. La manipulación y la interferencia con un sistema electrónico o informático está destinado principalmente para producir beneficios económicos para el usuario remoto.

A. Fraude

La mayoría de los países penalizan el fraude a través de Internet.

Hay algunas excepciones. En los Países Bajos, además de la pornografía infantil, no hay otros delitos relacionados con el contenido en función de la utilización de la tecnología de información y comunicaciones. Delitos relacionados con el contenido se consideran " tecnológicamente neutrales", lo que significa que lo que cuenta es la definición sustantiva del delito, con independencia de las modalidades utilizadas para cometerlos. En Rumania, no se indica explícitamente ninguna otra responsabilidad penal además de penalizar los delitos contra los derechos de autor. La legislación rusa tampoco es explícita al respecto. La legislación sueca no prohíbe sanciona específicamente el fraude a través del uso de las tecnologías de información y comunicación. En Japón, el fraude informático se introdujo en el Código Penal en 1987.

B. Violación de los Derechos de Propiedad Intelectual

La mayoría de los países reconocen la infracción de derechos de propiedad intelectual.

Algunos, como Alemania e Austria, adoptan e integran en su legislación la Directiva 2001/29/CE 3 de la Unión Europea, por ejemplo, en los artículos que protegen a las medidas técnicas, programas informáticos y etiquetas.

Bélgica, Luxemburgo y Japón no tienen disposiciones especiales para violaciones de la propiedad intelectual en y por medio de la Internet, pero se aplican las leyes generales de propiedad intelectual. Brasil, en general, no proporciona ninguna penalización de los actos en el mundo virtual. Además de la pornografía infantil, los Países Bajos no penalizan la comisión de un delito cometido en el mundo virtual cuando se trata de personas no reales. La ley holandesa tiene un enfoque diferente de muchos otros países a la pregunta: ¿Es un objeto virtual, un bien que puede ser robado? Según el Tribunal Supremo holandés, los datos no son bienes. Una cualidad esencial de los bienes, para que sean robados, es que la persona debe perder el control de ellos a otra persona que está ganando el control de ellos. Datos digitales carecen de esta propiedad, ya que pueden coexistir bajo el control de dos o muchas personas. Sin embargo, en el caso *Runescape* (2012), el Tribunal Supremo holandés dictaminó que los objetos virtuales en un juego de ordenador son bienes que pueden ser objeto de robo, siempre y cuando sean un objeto que se puede quitar desde el control de facto de otra persona. En el caso Runescape, una persona real cometió el robo en perjuicio de otra persona real.

Rumania sanciona delitos contra los derechos de autor. No otra responsabilidad penal es indicada explícitamente.

Rusia se unió a la Organización Mundial de la Propiedad Intelectual (OMPI) en 1996. La legislación rusa se ha actualizado para cumplir con los estándares internacionales para la protección jurídica de los derechos de autor. Artículos 146 y 147 del Código Penal de Rusia son aplicables a las infracciones cibernéticas. La legislación sueca, en cambio, no proscribe específicamente y no sanciona fraude y la violación de derechos de propiedad intelectual cometidos mediante el uso de tecnología de las comunicaciones de Internet. En los Estados Unidos, el fraude a través de un ordenador, la infracción de los derechos de propiedad intelectual y el tráfico de bienes y servicios falsificados están todos criminalizados.

C. Espionaje Industrial

Algunos países penalizan espionaje industrial: Dinamarca, Finlandia, Italia, Japón, sobre la base de disposiciones de carácter general (por ejemplo, la competencia desleal y las leyes de derechos de autor) ; Polonia sobre la base tanto de la protección de la propiedad intelectual como también de leyes para la lucha contra de la competencia desleal; Rusia, no específicamente pero en base a las disposiciones generales sobre la recogida ilegal de secretos comerciales; Turquía, Suecia, y los Estados Unidos proscriben el robo de secretos comerciales y el espionaje industrial.

5. La penalización de los actos cometidos en el mundo virtual

Los actos cometidos en el mundo virtual abren nuevas fronteras en el derecho penal y los principios y las definiciones tradicionales de prueba, como la de "bienes" (para la pornografía infantil virtual, ver más arriba). El discurso es acerca de las lesiones de mundos virtuales que requieren remedios en el mundo no virtual. Una discusión importante es si el mundo de Internet es bastante único para requerir su propia regulación y si ciertas acciones en Internet necesitan sus propias normas especiales y específicas. Hay quienes sostienen que, antes de aprobar los reglamentos excepcionales de internet, la sociedad debe comprender y explicar con claridad cómo las actividades de Internet son tan diferentes y / o especiales y por lo tanto por qué justificar sus propios reglamentos específicos. Una de las preguntas más profundas es la base y la fuente del derecho cibernético. Algunos consideran el ciberespacio como nuevo, independiente y apartado, capaz y autorizado para crear sus propias instituciones y articular sus propias leyes. Otros no ven cómo y por qué las transacciones por Internet son diferentes de las transacciones transnacionales del mundo real y por qué deben estar fuera del alcance de las regulaciones territoriales. En otras palabras, a través de Internet o de comunicaciones electrónicas, se hace un paso fuera del mundo "real " en un mundo virtual, que es igualmente real, con sus definiciones, normas y sanciones? ¿Toma uno un paso fuera de su propio país en una jurisdicción mundial o, algún día, espacial, sin fronteras, universal, aceptando implícitamente la jurisdicción de todos los países del mundo? También son especialmente complejas, nuevas y desafiantes las situaciones delictivas que involucran interacciones de Avatar a Avatar o las acciones de los robots.

La mayoría de los países encuestados no reconocen ninguna penalización en el mundo virtual: Argentina, Austria, Brasil, Finlandia, los Países Bajos (con excepción de la pornografía infantil, y con la salvedad de que no haya personas reales involucradas), Rumania, Rusia, Turquía y los Estados Unidos (a excepción de la

pornografía infantil). De todos modos, muchos países como Bélgica, Luxemburgo, Croacia, Dinamarca, Países Bajos, Suecia y los Estados Unidos criminalizan la pornografía infantil virtual.

Otros tipos de violencia virtual no son tan a menudo reconocidos como crímenes. Por ejemplo, en Bélgica y Luxemburgo, la violencia virtual no está incluida. La violencia sólo puede existir entre personas reales o contra los bienes reales. Sin embargo, el sabotaje y la piratería virtuales son criminalizados. Virtual grafiti no son punibles. Finlandia no tiene una disposición especial para los actos cometidos en el mundo virtual. La difamación y hostigamiento sexual cometidos en el mundo virtual se reconocen como delitos en algunos países como Suecia, Dinamarca, Bélgica y Luxemburgo. En Alemania, la difusión de material que contiene violencia virtual / ficción se penaliza como tal, cuando se glorifica la violencia o se minimiza o la dignidad humana es violada y también cuando hay violencia pornográfica. Para incluir la violencia virtual, el objeto del delito se ha extendido a los "seres humanoides. " La Ley penal alemana no penaliza expresamente grafiti virtuales. Cuando se trata de Avatares, no están protegidos de por sí. Debe existir un enlace, por ejemplo, en el caso de un insulto personal, con una persona física para que un crimen pueda existir. Lo mismo se aplica en el caso de acoso sexual.

6. Delitos de no cumplimiento

Informes recientes y revelaciones de Wikileaks y en especial por Edward Snowden han proporcionado una visión no sólo de los grandes programas usados por algunos gobiernos para interceptar, registrar, escuchar, almacenar y analizar las comunicaciones personales y de negocios de los ciudadanos y extranjeros, sino también del alto nivel de cooperación entre los proveedores de servicios de Internet (ISP) y la policía y las agencias de inteligencia en muchas partes del mundo. Algunos proveedores de servicios de software y de Internet (ISP) ofrecieron de ayudar a las fuerzas del orden para eludir sus propios sistemas de cifrado mientras mantienen la pretensión de que ellos valoran y protegen la privacidad de sus clientes. Por lo tanto, existe un considerable escepticismo actual respecto a las promesas de privacidad y garantías que proveedores de servicios de Internet ofrecen para el consumidor y el ciudadano. Hay una sensación de que estas políticas de privacidad son herramientas de marketing sin valor y promesas vacías que pueden ser fácilmente burladas y esquivadas para fines de inteligencia y policía, así como para obtener ganancias económicas mediante la extracción de datos y la venta de información relacionada con la comercialización y marketing. Los llamados "medios sociales " especialmente constituyen un depósito masivo de informaciones sobre estilo de vida, compras, viajes, gastos personales que se extraen y se venden a varias empresas para centrar su mensaje de ventas hacia sus clientes más probables. Lo mismo puede decirse de los programas de fidelidad de las aerolíneas, supermercados, varias tiendas, cines, librerías, entre otros.

Como declaración general sobre la materia, la defensa nacional, la seguridad del Estado y el orden público tienen prioridad sobre la privacidad y los derechos humanos y civiles. Todos los países, de forma y grado ligeramente diferente, requieren la cooperación con la policía, la retención de datos, por lo general durante al menos 6 meses, a veces por un año (Dinamarca), el bloqueo de las comunicaciones a petición de las autoridades, dar acceso a los sistemas informáticos para instalar los dispositivos necesarios para la recogida en tiempo real de los datos de tráfico y la interceptación de datos de contenido. El incumplimiento puede resultar en cargos de desacato, la detención, el encarcelamiento, sanciones administrativas o multas. La ley belga y luxemburgués no penalizan específicamente la falta de cooperación en la materia. Sin embargo, un juez puede requerir ciertas personas para que cooperen y hay sanciones penales por no hacerlo. En Japón, hay muchos delitos de incumplimiento y el campo de la delincuencia informática no es una excepción con multas como sanción. Alemania también requiere que los proveedores de servicios cooperen con las autoridades y proporcionen la información solicitada sin demora. Si hay una objeción, la policía y los fiscales pueden usar varias herramientas regulatorias y coercitivas a su disposición. Negar información solicitada puede constituir un delito. No hay información sobre este tema a través de los informes de Brasil, Turquía y Argentina. Rusia no tiene disposiciones específicas. Algunos países, como Finlandia, limitan el castigo por el incumplimiento a las multas. Italia prevé sanciones administrativas, a pesar de que el incumplimiento posiblemente puede llegar a ser un delito. En los Estados Unidos, existen sanciones penales por no mantener los registros relacionados con la producción de material sexualmente explícito. En la mayoría de los casos, los investigadores deben presentar una citación judicial. El incumplimiento puede dar lugar a desacato civil, arresto, encarcelamiento y multas. Un testigo recalcitrante puede ser encarcelado por no más de 18 meses en total.

Un tema de creciente preocupación y debate es la obligación de reportar los delitos cibernéticos conocidos. De acuerdo con el informe polaco, las personas que tengan información sobre un delito cibernético punible

deben notificar a las autoridades. Existen sanciones por no presentación de informes. En general, los demás informes nacionales no abordan esta cuestión, que es, sin embargo, inevitable y que, finalmente, hay que abordar.

Conclusión

El derecho penal puede y debe desempeñar un papel crucial para hacer frente a la rápida evolución y siempre cambiante fenómenos relacionados con el mundo cibernético, el ciberespacio, las redes sociales y las comunicaciones en todo el mundo electrónico.

En este sentido, es esencial plantear aquí la cuestión de los derechos humanos; la libertad de expresión; la expresión artística; la dominación cultural de los países desarrollados; los intereses financieros en el control de la creación, la comercialización, el acceso y el uso de la información; el autoritarismo o sus vestigios que permiten limitar la libertad de comunicación de las personas; la expresión y el intercambio de información bajo la amenaza de ser acusado de difamación de funcionarios públicos; la supuesta falta de respeto a las instituciones del Estado, las fuerzas armadas, la policía, etc.

También es importante tener en cuenta las diferentes tradiciones jurídicas cuando se trata de la libertad de expresión, los límites de la expresión de opinión y de los valores de uno antes de desencadenar sanciones penales; el uso de la censura para silenciar la crítica y frenar la innovación; el ángulo de lucro que puede motivar conglomerados privados de entretenimiento, música, actuación y artes creativas de acabar expresiones artísticas innovadoras que pueden cortar en sus beneficios o impugnar su dominación cultural, lingüística y artística o la de algunos países, etc.

Está claro que el uso del derecho penal puede ser positivo, protegiendo los intereses valiosos y legítimos, o negativo, apoyando a regímenes autoritarios y a valores y prácticas culturales y religiosas que pueden ser consideradas asfixiantes y opresivas.

La invocación de "derechos humanos, religiosos, culturales" no es siempre una justificación automática o suficiente para sanciones penales, la censura y las limitaciones en las expresiones personales, políticas y artísticas. Por lo tanto, la demanda de una mayor criminalización y penalización debe ser cuidadosamente considerada y equilibrada. Al inicio se consideró el Internet como finalmente el verdadero mercado libre de ideas y comunicaciones. Desde entonces, ha habido un esfuerzo concertado por parte de regímenes autoritarios y también democráticos para limitar, controlar, explotar, silenciar, y castigar lo que está siendo publicado y distribuido a través de Internet. Es la responsabilidad de la AIDP de evaluar de forma prudente, equitativa y justa las afirmaciones contrastantes y proponer soluciones y enfoques equilibrados que tengan en cuenta la diversidad, las diferencias culturales y religiosas, la expresión literaria y artística y una buena dosis de desconfianza hacia mirar siempre al derecho penal y al estado como la solución para todos los problemas.