Ius Comitiãlis
ISSN: 2594-1356
iuscomitialis@uaemex.mx
Universidad Autónoma del Estado de México
México

Piña Libién, Hiram Raúl
Cibercriminalidad y ciberseguridad en México[1]
Ius Comitiãlis, vol. 2, núm. 4, 2019, Julio-Diciembre, pp. 47-69
Universidad Autónoma del Estado de México
México

DOI: https://doi.org/10.36677/iuscomitialis.v2i4.13203

Cibercriminalidad y ciberseguridad en México[1]

Cybercriminality and cybersecurity in Mexico

Hiram Raúl Piña Libién*

Ius Comitialis / Año 2 Número 4 / julio-diciembre 2019 / pp. 47-69 / ISSN 2594-1356
Recepción: 04 de junio de 2019 / Aceptación: 16 de octubre de 2019

Resumen

El presente trabajo explora la ciberdelincuencia desde un punto de vista hermenéutico y conceptual. Analiza las políticas públicas y legislación que en materia de sociedad de la información y ciberseguridad se han implementado en México; así como la jurisprudencia que se ha emitido respecto a la colisión entre libertades fundamentales y el uso indiscriminado de la informática. Su propósito es presentar el panorama epistemológico para el entendimiento de la delincuencia informática, ante la posibilidad de que México pueda adherirse a la Convención de Budapest.

Palabras clave

Ciberdelincuencia, cibercriminalidad, política informática, legislación informática, delito informático.

Abstract

The present work explores cybercrime from a hermeneutic and conceptual point of view. Analyze public policies and legislation that in the field of information society and cybersecurity have been implemented in Mexico; as well as the jurisprudence that has been issued regarding the collision between fundamental freedoms and the indiscriminate use of information technology. Its purpose is to present the epistemological panorama for the understanding of computer crime, given the possibility that Mexico may adhere to the Budapest Convention.

Key words

Cybercrime, computer policy, computer legislation, cyberlaw, intertet law.

*Profesor de tiempo completo definitivo por oposición en la Facultad de Derecho de la Universidad Autónoma del Estado de México. Consejero ciudadano del Sistema Municipal Anticorrupción de Toluca, México. ORCID: https://orcid.org/0000-0002-5745-6880. Correo electrónico: hrpl@hotmail.com

[1] El presente trabajo tomó como base parte de la obra *El derecho a la autodeterminación informativa y su garantía en el ordenamiento jurídico mexicano*, del mismo autor, ampliando la discusión sobre el tema.

INTRODUCCIÓN

Una nueva civilización está emergiendo en nuestras vidas, y hombres ciegos están intentando en todas partes sofocarla. Esta nueva civilización trae consigo nuevos estilos familiares; formas distintas de trabajar, amar y vivir; una nueva economía; nuevos conflictos políticos, y más allá de todo esto, una conciencia modificada también.

Alvin Toffler
La Tercera Ola

El Derecho es una ciencia que tiene como fin regular situaciones jurídicas concretas a través de supuestos contenidos en la norma. Su proceso de creación y actualización depende de diversos mecanismos, no solamente del proceso legislativo como forma ordinaria de creación; los usos y costumbres observados en determinada época y sociedad posibilitan su actualización.

Desde la segunda mitad del siglo XX ha existido un enorme avance científico y tecnológico; la liberación de las computadoras transformó el contexto laboral, social político y económico de los países en todo sentido. La irrupción y masificación de la informática y las telecomunicaciones han traído consigo una revolución en diversos ámbitos, dentro de los cuales, el jurídico no ha sido la excepción. La reconcepción de figuras jurídicas añejas como la del comercio, es muestra del impacto que las Tecnologías de la Información y la Comunicación (TIC) han ejercido en las últimas décadas sobre la sociedad y el Derecho.

El problema de las TIC y sus aspectos legales se presenta como un campo fecundo no sólo en el ámbito de la producción jurídica; sino también, en su filosofía e investigación teórica; por ello, este trabajo tiene como propósito discurrir sobre el panorama teórico-jurídico de las conductas criminales informáticas en el marco de la Sociedad de la Información (SI), así como exponer la política informática y el marco jurídico mexicano vigentes que les son aplicables.

LA SOCIEDAD DE LA INFORMACIÓN

Si damos por sentado que el Derecho es un sistema de normas que se hacen valer por medio de la fuerza o que reglamentan el uso de ésta dentro de un conglomerado

social (García, 1999, p. 14), debemos aceptar también, que las normas dimanantes del Derecho deben ser obedecidas por sí mismas. Esta concepción positivista del Derecho hace ver que el sistema de normas debe hacerse valer por el Estado y respetado por el conglomerado social, en virtud de que la norma jurídica es general, abstracta, coercible, heterónoma, provista de una sanción legal y tendente a la búsqueda del bienestar social.

El Derecho, al constituirse como un medio de control social, marca la diferencia que existe entre Derecho y Moral; que se concreta en que el Derecho regula las relaciones externas de los hombres (Bodenheimer, 1994, pp. 94-95) y en cambio, la moral se reduce a un aspecto meramente interno del hombre en particular, exigible a sí mismo, sin efectos exteriores que se reflejen por su transgresión o incumplimiento.

En caso de que la norma jurídica sea violada, ésta impone al transgresor o incumplidor la sanción señalada por el Estado creador de esa norma, para resarcir mediante una pena, el daño hecho a la sociedad. Por sí misma, la disposición legal pide un absoluto sometimiento a sus normas y mandamientos, sin tener en cuenta si determinado individuo la aprueba o no; y se caracteriza por el hecho de que lleva siempre consigo la amenaza de la coacción física (Bodenheimer, 1994, pp. 94-95).

El Derecho tiene diversos sentidos. En sentido objetivo, se entiende por derecho al conjunto de normas provistas de sanciones que rigen las relaciones de los hombres en sociedad y, en sentido subjetivo, la prerrogativa perteneciente a una persona, que le permite exigir de otra, prestaciones o abstenciones (derechos personales), o el respeto de una situación en la que ella aprovecha (derechos reales y derechos individuales).

No puede, ni debe darse por hecho, que el Derecho es un conjunto de normas fijas y obsoletas; por el contrario, es cambiante y dinámico, se transforma con el paso del tiempo y se adecúa a las necesidades de la sociedad, debido a los diversos fenómenos que surgen como consecuencia de la evolución del hombre; lo que se traduce en un distanciamiento entre el mundo del ser y del deber ser, es decir, entre lo que es la norma escrita y lo que es la realidad.

La distancia entre la realidad y la pretensión jurídica de la eficacia social, a través de un sistema de equidad y justicia, basado en un conjunto de normas, se dificulta en gran medida, debido a que:

> El cambio social y el mero hecho del cambio social tienen un impacto dramático, fundamental, en la cultura de la sociedad moderna; influye en la manera de pensar de la gente, así como en la forma en que viven. Ha habido una revolución en las expectativas sociales, el público moderno está acostumbrado al cambio y, (...) es en parte por esa razón que no es indiferente y fatalista, sino, en realidad, infinitamente demandante. La personalidad del hombre moderno, (...) es diferente en aspectos fundamentales (...) la tecnología es, al menos en parte, responsable de estos cambios (Friedman, 1993, pp. 55-57).

Hoy día, en cualquier área productiva se encuentra a la tecnología como un factor de cambio. El Derecho, como se ha señalado, no es un conjunto de disposiciones

fijas y obsoletas, y en gran medida las TICs son elementos que permiten su reconfiguración.

Las TIC no sólo son factor de replanteamiento del Derecho, también de la estructura de la sociedad, pues con la masificación del denominado ciberespacio,[2] se está gestando la SI, en donde todas las personas nos podemos ver afectadas por las TIC, mismas que representan una nueva forma para que el Estado ejerza su poder.

Esta sociedad, tanto en la expresión coloquial como en definiciones académicas, se refiere al impacto global y al conjunto de las transformaciones que están produciendo en la organización social y en la vida individual las nuevas tecnologías de la información y la comunicación (TIC) (Carrascosa, 2003, p. 9).

Yoneji Masuda elaboró un modelo de SI que puede ser visto como un "Estado automatizado", el cual debe entenderse como una organización política totalitaria apoyada en el control tecnológico, la Computopía (*computer-based utopia*), es decir, la sociedad libre a través de las computadoras y de la información (…) será por tanto, una sociedad sin clases libre de un poder dominante, cuyo núcleo social serán las comunidades voluntarias (Pérez Luño, 1987, p. 143). Comprendido así, el "Estado automatizado" de Masuda, éste tendrá como eje los valores cognoscitivos, más que los valores materiales (Pérez Luño, 1987, p. 39).

Simon Nora y Alain Minc (1980, pp. 26-27) la describen como una sociedad adulta, que desarrolle su espontaneidad, su movilidad y su imaginación, aceptando al mismo tiempo las responsabilidades de la normativa universal; pero también supone un Estado que, asumiendo sin timidez sus funciones reguladoras, admite, sin embargo, no seguir siendo el actor casi exclusivo del juego social.

Esta sociedad se configura, debido a que las TIC son accesibles, rápidas, económicas, abiertas y globales, sin limitación de fronteras territoriales, políticas y culturales; permitiendo con ello diseminar y difundir los datos e información, a través de redes de datos.

No obstante, cabe agregar que es el resultado de un vasto y complejo proceso de transformación de las sociedades industriales. El concepto pretende indicar la importancia preeminente que tiene la información en la vida social actual (Fix Fierro, 1990, p. 46).

Puede concluirse que la SI es un fenómeno de retos y oportunidades, incertidumbre y caos, resumible en la hipótesis de que es la occidentalización de la sociedad basada en la información; pues valores como la democracia, la transparencia, la seguridad nacional e internacional, así como el flujo e intercambio de información y mercancías, se presentan como la única vía o alternativa para el desarrollo humano y social, lo que es posible realizar mediante la utilización de las TIC.

Pero no todo es optimismo en la SI, cuya punta de lanza es Internet. En su interior, se ha creado un submundo de ocio y diversión, de intercambio de información de toda índole, que va desde aquella de carácter científico, político, cultural y personal, hasta el pornográfico. En esta interioridad de la SI, lograda por el ciberespacio, la información se trasmite sin limitación de fronteras, sin conocimiento de su veracidad y peor aún, con escaso control de las autoridades estatales. En su exterior, ha convertido al hombre en Tecnófilo (Postman, 1994, p. 5), pues supone que lo más tecnológicamente avanzado es lo mejor (Graham, 2001, p. 21), es decir, nos encontramos inmersos en nuestra aventura amorosa con las máquinas que intervienen en nuestras vidas (Roszak, 1990, p. 62).

[2] Es importante señalar que se trata de un ambiente intangible; no es un mundo de átomos y células, sino digital (Goodman, 2003, p. 8).

Aparentemente estamos en un callejón sin salida, por una parte el ciberespacio es un lugar sin límites y con escasos controles; pero por otro, día a día nos deslumbra con sorprendentes innovaciones y adelantos científico-tecnológicos.

La respuesta a las inquietudes que puedan plantearse con respecto a los beneficios y perjuicios que trae consigo la SI, sólo tiene cabida en la reflexión filosófica que se haga de ella, con el objeto de darle significación y explicación en sus aspectos económico, político, cultural y democrático.

Si reflexionamos bajo un prisma filosófico, respecto de las bondades y maleficencias de la revolución informática, podremos dilucidar una filosofía de la informática y una filosofía informática.

La informática es una herramienta de innumerables aplicaciones. Actualmente, se encuentra presente en muchas de las actividades diarias de la sociedad moderna. Esta valiosa herramienta no solamente se reduce al uso de computadoras y redes de datos; la informática tiene múltiples aplicaciones científicas, económicas, políticas y sociales, como el permitir que el flujo vehicular de las grandes ciudades sea más ordenado mediante la sincronización de semáforos. A través de la informática es posible la detección y tratamiento de enfermedades y padecimientos crónico degenerativos, a través de mecanismos especializados, como la tomografía computarizada y los respiradores artificiales para pacientes con afecciones respiratorias; en la vigilancia y seguimiento del producto de la concepción humana, a través del ultrasonido; el diagnóstico por computadora, la realización de historias clínicas, el procesamiento de imágenes, así como el proyecto del genoma humano.

Otras aplicaciones de la informática se dan, por ejemplo, en la ingeniería civil al proveer herramientas que mejoran la construcción y los cálculos; en el diseño estructural y en la topografía y movimiento de tierras; dentro de la arquitectura, en la realización de planos y maquetas tridimensionales, creación de logotipos o figuras distintivas; en la administración de oficinas en el ámbito de la ofimática.

Así, podrían mencionarse un sinfín de aplicaciones y realizar una lista más exhaustiva, la que resultaría obsoleta al poco tiempo, pues el constante cambio e innovación tecnológica, convierten al más sofisticado avance en tecnología rudimentaria, logrando con ello el sueño eterno del *Tecnófilo*, quien alberga esperanzas sobre un mundo mejor. Si se prefiere, también se le puede llamar *quietista*.

Como puede verse, la informática ha modificado el esquema social, tornándolo más frío y distante de los valores que le dan sustento; lo afirmamos, puesto que el hombre se ha visto enajenado por la tecnología y sus avances. La aplicación de la informática en la sociedad debe reducirse a un proceso de informatización responsable y no convertirse en una prótesis económica, social y cultural del hombre, ésta es la filosofía de la informática.

En lo que respecta a la filosofía informática, puede decirse que ésta se centra en su correcto uso y aprovechamiento. El desmesurado uso y aplicación de la informática genera en lo particular y en lo colectivo, la pérdida de la identidad y la generación de los vicios humanos; en consecuencia, el hombre se torna irracional y autómata.

Recordemos cómo en los albores de la Revolución Industrial, un grupo de individuos comandados por Ned Ludd se dieron a la tarea de destrozar la maquinaria que amenazaba con sustituirlos en las fábricas, por considerar que ponían en peligro su trabajo y su subsistencia. Quiénes también se opusieron férreamente a la introducción de aparatos en sus fuentes de trabajo, fueron los sastres, ya que destrozaron las máquinas de coser inventadas por Barthelemey Thimonnier. Ellos fueron abier-

tos combatientes de la innovación tecnológica y han sido conocidos como *ludditas*. Si se prefiere, también se les puede llamar *nihilistas*.

En el campo económico, la informática ha venido a reducir el proceso de comercialización de mercancías, mediante el llamado *e-Commerce*, en donde comprador y vendedor se encuentran en lugares distantes de la geografía mundial; pero ésta no es ni será la única repercusión económica de la informática; el poderío de las empresas informáticas pone de manifiesto esta situación. Otra importante repercusión de la informática en el ámbito económico es el empleo, ya que la tecnología ha venido a sustituir la mano de obra, generando con ello desempleo y pérdida del poder adquisitivo.

El aspecto político de la informática radica en la apertura de oportunidades y la generación de expectativas más reales para la sociedad. La informática pretende generar una democracia de acceso a los medios de comunicación e información; en un solo sentido, que todos los ciudadanos tengan a su alcance información pronta, objetiva y veraz de manera oportuna.

Puede decirse que, el hombre está afectado por el avance tecnológico más que nunca antes y las posibilidades de personalización se ven reducidas cualitativamente porque los valores de la persona se esfuman, y cuantitativamente porque los hombres son masificados y sólo un número reducido es el que puede beneficiarse sin dañarse (Parent Jacquemin, 1986, p. 25).

Los altos costos y difícil acceso a la tecnología hacen que, en vez de hablar de una democracia informática, estemos, por una parte, ante la presencia de un proceso de dominación y sujeción intelectual, económica, política, social y cultural, y por otro, ante una actitud reticente para adoptar y adaptar racionalmente la tecnología a nuestras actividades cotidianas. En el primer caso se presenta *l'homme infomatique*, al que Vittorio Frosini identifica como *l'uomo artificiale*; en el segundo caso, estamos ante la presencia de los *neoludditas*. Pero algo es cierto y contundente, y es el hecho de que, los últimos desarrollos de la ciencia y de la técnica, que surgieron como fuerzas emancipatorias de la humanidad, constituyen ahora una amenaza de dominio y de opresión (Pérez Luño, 1987, p. 44).

De ahí que deba realizarse una la evaluación para saber cuál es el papel que juegan las TIC en la SI. Consideramos que el retorno a lo ético es en parte, solución a este problema de la filosofía informática; y estamos convencidos de que la ciencia jurídica tiene más que nunca, un rol trascendental para el futuro de la humanidad, para que ni el *neoluddismo* ni la *Tecnófilia* nos absorban; por ello, es necesario plantear que el Derecho debe ser un medio para la debida racionalización de las TIC y su correcta aplicación en la SI.

En síntesis, la filosofía informática se concreta en la generación de un proceso de informatización ético y responsable, en donde cada usuario de las TIC, conscientemente las adopte y dinamice su uso y, a la vez, le permitan su integración en la SI.

No obstante, esta aspiración teleológica, debemos reconocer que hoy día nos encontramos inmersos en la que bien puede llamarse la era de la personalización, caracterizada por un filtro burbuja (Parisier, 2017), que se encuentra instalado en cada ordenador y dispositivo móvil que se enlaza a Internet, es decir, contamos con una red predictiva y persuasiva, basada en algoritmos que recopilan información sobre los usos, intereses, accesos y comportamientos de los usuarios de Internet, para posteriormente influir mediante sugerencias de lo que debe o presuponen le interesara ver o consultar en un futuro mediato, alterando con ello nuestra manera de encontrar ideas e información (Parisier, 2017, p. 19).

Como puede atisbarse, los filtros que constituyen diversas burbujas, además de determinar nuestro consumo de información, potencializar el comercio electrónico y determinar nuestra interacción individual y grupal, especialmente a través de las redes sociales, nos torna solitarios, invisibles y absortos del mundo exterior, pues nos sesgan para descubrir nueva información –atendiendo como referencia a los previos consumos–, produciendo en lo mediato imparcialidad, falta de objetividad y ausencia de veracidad para el encuentro de futuras informaciones.

En lo que decidimos por alienarnos entre ser ciberescépticos o cibervisionarios, entre contar con una ciberciudadí@ o desarrollar una ciudadaní@.com (Pérez Luño, 2004, p. 100), o debatimos si pertenecemos a una determinada legión de idiotas (Eco, 2016, pp. 492-493) en la sociedad algorítmica, somos atropellados por los altísimos costos personales, culturales y sociales que el filtro burbuja produce a nuestra personalidad y el futuro social-global, aún a costa de que otros decidan por nosotros; de ahí que, existan riesgos para los derechos humanos, la política y la democracia en el Estado constitucional.

Para entender los riesgos a los que se encuentran expuestos los derechos humanos en la sociedad tecnológica, debemos tener en cuenta que los seres humanos no somos nodos virtuales de las redes sociales, por mucho que los *nerds* y los *geeks* lo pretendan. En el mundo virtual, las personas pueden optar por comportarse como seres infrahumanos, pero la red social no es el mundo real de la sociedad (Wark, 2011, p. 79). La exposición de los seres humanos en el mundo virtual ha tenido como consecuencia negativa que las relaciones interpersonales se destruyan. Ello se debe, en gran medida, al uso indiscriminado de las redes sociales, exacerbado nuestra capacidad para asumir conductas, roles o personalidades ficticios, es decir, fingir y proyectar en el ciberespacio todo aquello que siempre quisimos ser en la vida real, pero que jamás pudimos realizar debido a nuestras limitaciones. Es indudable que las redes sociales además de estimular la frialdad emocional y potencializar los trastornos de identidad disociativa, violentan y separan invisiblemente a los seres humanos. Los costos de consumir información irrelevante, se traducen en tener menos margen para el intercambio de ideas y vivir una vida dentro de una burbuja de filtros que funciona como mecanismo de autopropaganda y escaparate para denotar una aparente vida feliz (Parisier, 2017, pp. 22-24).

En el plano político-democrático, bien vale la pena citar la alianza realizada entre Facebook Ireland Limited y el Instituto Nacional Electoral (INE), quienes el 3 de febrero de 2018 signaron un Memorándum de Cooperación (MoC), que si bien expresamente no constituye ni crea obligaciones vinculantes u obligatorias entre ambas partes, sí prevé la cooperación de la primera para que algunos de sus productos de participación ciudadana estén disponibles en su plataforma para sus usuarios en México, en tanto que el segundo, le proporcionara el día de la jornada electoral, información en tiempo real sobre los resultados de la votación que se generen a través del Programa de Resultados Electorales Preliminares.

Ningún cuestionamiento jurídico o suspicacia política tendría la posibilidad de que ambas partes celebraran foros y eventos relacionados en general con las elecciones –como se estableció en el apartado 3 del convenio–, tales como sesiones de aprendizaje para periodistas respecto a cómo se organizan y celebran las elecciones en México, sin embargo, debe decirse que el MoC, además de haber sido redactado con ambigüedad jurídica respecto a su objeto, quedó en tela de juicio al no encontrarse fundamentado en las disposiciones legales aplicables, sino sujeto a la Declaración de Derechos y Responsabilidades de Facebook, incluyendo todas las políticas y guías a las que hace referencia, es decir, a las condiciones del servicio que

rigen a Facebook con cada usuario, mismas que le posibilitan para que pueda retirar cualquier contenido o información que se publique, si tal empresa considera que se infringe esa Declaración o sus políticas de servicio.

LA CIBERDELINCUENCIA

La doctrina no ha tenido un criterio uniforme respecto a la conceptualización del *Computer Crime*, así por ejemplo, encontramos que se ha sostenido que es aquel conjunto de conductas criminales que se realizan a través de del ordenador electrónico, o que afectan el funcionamiento de los sistemas informáticos (Pérez, 1996, p. 70), o la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (Davara, 1993, p. 318).

En nuestra opinión, la *Computerkriminalität* es una conducta ilícita que jurídicamente es reprochable; puesto que busca dolosamente, por una parte, vulnerar bienes jurídicos relacionados con la informática, en sus aspectos lógicos y físicos, y por otra, atentar y restringir los derechos y libertades individuales fundamentales. En suma, son conductas criminales que se caracterizan por ser altamente tecnificadas y con incalculables repercusiones económicas.

La actualización de los ordenamientos jurídicos penales en materia de delitos informáticos ha sido influenciada por la Convention on Cybercrime, firmada en Budapest el 23 de noviembre de 2001. A través de este convenio, los Estados miembros del Consejo de Europa establecieron una política penal común destinada a prevenir la criminalidad en el ciberespacio, mediante la adopción de una legislación apropiada y la mejora de la cooperación internacional.

De otra parte, en el ámbito del derecho penal internacional de los delitos informáticos, se encuentran las resoluciones de la Organización de las Naciones Unidas (ONU): 55/63 de 4 de diciembre de 2000 y 56/121, de 19 de diciembre de 2001, sobre el establecimiento de la base jurídica para luchar contra la utilización de las tecnologías de la información con fines delictivos; 53/70 de 4 de diciembre de 1998, 54/49 de 1° de diciembre de 1999, 55/28 de 20 de noviembre de 2000, 56/19 de 29 de noviembre de 2001, y 57/53 de 22 de noviembre de 2002, sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional; y, la 57/239 de 20 de diciembre de 2002, a través de la cual se busca la creación de una cultura mundial de seguridad cibernética.

Sobre la base de esta última resolución, se pretende que los Estados miembros de la ONU sean por una parte, conscientes de la necesidad de la seguridad de los sistemas y redes de información y de lo que pueden hacer por mejorarla; y de otra, ser responsables de la seguridad de esos sistemas y redes de información en cuanto corresponde a sus funciones individuales, debiendo para ello examinar periódicamente sus políticas, prácticas, medidas y procedimientos, a fin de evaluar si son las que convienen en su contexto.

En este contexto internacionalista, la Cumbre Mundial de la Sociedad de la Información (CMSI) constituyó la primera negociación multilateral en cuya prepa-

ración participaron de igual a igual, organizaciones no gubernamentales, gobiernos, empresas y sociedad civil; tuvo como objetivo la adopción de políticas para superar la brecha digital, es decir, para abatir desigualdades entre países ricos y pobres en el acceso Internet y las TIC.

La CMSI en sus dos fases de desarrollo, se constituyó como el foro global en el que se delinearon las políticas internacionales para la implementación y seguimiento de la SI, así como para el establecimiento de una agenda multilateral orientada a establecer mecanismos para la financiación de las TIC y la gobernanza de Internet.

No obstante que los compromisos establecidos en la CMSI están fundamentalmente orientados a abatir las desigualdades existentes entre países ricos y pobres en el acceso a Internet y las TIC, lo cierto es también que, se reconoció la necesidad de evitar que se abuse de las tecnologías y de los recursos de la información para fines delictivos y terroristas, respetando siempre los derechos humanos.

Estamos convencidos de que la SI debe promover la justicia, así como la dignidad y el valor de la persona humana, el fomento y respeto de los derechos humanos y las libertades fundamentales de otros, incluyendo la privacidad personal y el derecho a la libertad de opinión, de conciencia y religión. Por ello, la adopción de las medidas preventivas y las acciones necesarias para su desarrollo debe realizarse con arreglo a la legislación, a fin de impedir su utilización abusiva que da lugar, entre otros, a actos ilegales motivados por el racismo, la discriminación racial, la xenofobia, y la intolerancia, el odio, la violencia que ello entraña, todo tipo de abuso infantil, incluyendo la pedofilia y la pornografía infantil, así como el tráfico y la explotación de seres humanos.

Los ataques a los derechos y libertades fundamentales, en la era de la revolución informática, se presentan como lo afirma Javier Bustamante (1999, p. 167), de manera invisible, pues su inmaterialidad les hace escapar del escrutinio público.

Así, distintos regímenes políticos buscan mantener su estabilidad política, preservar los valores sociales, culturales, espirituales e históricos de sus sociedades, limitando el ejercicio de las libertades de opinión y expresión en Internet, y actuando en el marco del derecho penal en contra de sus detractores informáticos o ciberactivistas.

En el Informe de Amnistía Internacional (2018), se señala que países como Brunei Darussalam, Chad, China, Gabón, la región del Kurdistán en Irak, Kuwait, Líbano, Senegal, Tailandia, y Zimbague son países en los cuales se penaliza la expresión de comentarios vertidos en redes sociales o aquellos realizados a través de contenidos informativos y periodísticos, por considerarse que atentan en contra del régimen de gobierno y/o los detentadores del poder.

En muchos casos, los ciberactivistas alrededor del mundo, han sido encarcelados y enjuiciados por delitos como sedición, por revelar actos de corrupción a través de redes sociales, o bien, *so pretexto* de poner en peligro la seguridad nacional.[3]

Sobre esto último aspecto, destaca la política de cibersoberanía que el presidente Xi Jinping ha urgido asuma la comunidad internacional, entendiéndose por esta a la obligación de las naciones para respetar el derecho de cada país a elegir su propio camino hacia el desarrollo cibernético, modelo de regulación cibernética y participar en iguales condiciones (CNN, 2017).

[3] Ejemplo de lo anterior es la sentencia emitida por la Audiencia Nacional de España, en la que concluyó que los tuits del *rapero* Pablo Rivadulla Duró –conocido artísticamente como Pablo Hasél–, eran aptos para condenarlo, por segunda ocasión, por apología del terrorismo; así como también, la condena formulada por el Tribunal Supremo en contra del rapero Valtonyc por enaltecimiento del terrorismo e injurias a la Corona.

Para llevar a cabo esta política, el gobierno chino estableció en 2014 la 中央网络安全和信息化领导小组 (Oficina del grupo líder central para asuntos del ciberespacio), cuya función es regular, censurar, supervisar y controlar el flujo de información en Internet. Esta última circunstancia, implica la regulación, vigilancia y censura del contenido de los sitios web, tanto públicos como privados, ya sea en Internet visible como en Internet profundo.

En otras latitudes del mundo, la situación es hasta cierto punto contrastante de lo anterior. Verbigracia, los países que integran la Comunidad Económica de los Estados de África Central, en 2014 firmaron un instrumento regional denominado Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales, que en opinión del grupo de expertos sobre ciberlegislación y regulación para promover el comercio electrónico de la ONU, constituye un enfoque cualitativo para crear un marco jurídico digno de confianza [que] requería la gestión proactiva de los riesgos digitales, la aplicación efectiva de la ciberlegislación, el establecimiento de mecanismos de evaluación y vigilancia y la mejora continua del entorno propicio (Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, 2015).

En este contexto de tensión entre ciberseguridad, cibersoberania, ciberactivismo y la acción social pro defensa de los derechos humanos, México no se encuentra ausente en el Informe de Amnistía Internacional (2018, p. 312), por el contrario, ocupa un lugar especial en la agenda de preocupaciones de esta organización no gubernamental internacional, pues a propósito del *malware Pegasus*, a través del cual se presume se realizó el espionaje sobre periodistas, activistas sociales y defensores de derechos humanos, sentencia que en el periodo que abarca el informe, en México los ciberataques y la vigilancia digital eran especialmente habituales.

LA POLÍTICA DE CIBERSEGURIDAD EN MÉXICO

La sociedad informatizada (Zavala Alardín, 1990, p. 20) ha demandado el establecimiento de parámetros de planeación estratégica que permitan a los Estados y a los individuos su dirección e inserción. En este sentido, la política informática conforma el conjunto de directrices orientadas al desarrollo de la industria informática; la aplicación de las nuevas tecnologías de la información y la comunicación en el sector gubernamental con el propósito de vincularse con la ciudadanía y en el mejoramiento de la administración pública y los servicios que presta; así como para planificar el impulso, desarrollo y consolidación de los individuos en la SI.

En los albores de la revolución informática, la política informática se limitaba a la regulación de los estándares industriales que permiten la fabricación, distribución, importación y exportación de equipos, programas y consumibles de cómputo, es decir, se trata de una regulación basada en estándares tecnológicos.

Con el advenimiento del ciberespacio y la multiplicidad de interacciones que se dan en su seno, evolucionó como un mecanismo de autorregulación, es decir, como un sistema que tiene como uno de sus rasgos distintivos la participación de los grupos concernientes y de la sociedad en general (Moles, 2004, p. 219). Es decir, es un mecanismo de autocontrol y autodeterminación basado en un código deontológico compartido.

En el desarrollo presente y futuro de la SI, la política informática implica la intervención del Estado para que funja como ejecutor de las directrices y programas que se establezcan a través de un instrumento de planeación estratégica orientado a la informatización de la sociedad, es decir, para lograr la inserción cuantitativa de los ciudadanos en el imparable desenvolvimiento de la infraestructura de telecomunicaciones, así como el establecimiento de los mecanismos y herramientas necesarias para generar seguridad en la red.

Vale decir que, desde un punto de vista de política comparada, México se insertó con muchos años de retraso en la vorágine que conlleva el entendimiento, desarrollo y establecimiento de una política pública orientada a la informatización de la sociedad y sobre todo de ciberseguridad. Por ejemplo, el gobierno francés del presidente Valéry Giscard d'Estaingen (1974-1981), con el propósito de encontrar respuesta a los agravantes y graves desafíos, y superar las tensiones interiores de la sociedad francesa, encomendó a Simon Nora (1980, p. 7) un par de tareas: explorar y proseguir la reflexión sobre los medios de conducir la informatización de la sociedad, y, demarcar con mayor precisión el campo de estudio y la naturaleza del mandato que pudiera confiarse a una eventual comisión.

El resultado de la encomienda decanto en un informe, en el cual el Inspector General de Finanzas francés –junto con Alain Minc–, arribó a la conclusión de que las civilizaciones modernas, requieren del equilibrio y dosificación entre un ejercicio cada vez más vigoroso, aunque haya que limitarlo, de los poderes soberanos del Estado, y una creciente exuberancia de la sociedad civil (Nora y Minc, 1980, pp. 9-10).

Sin considerar que la inserción de los mexicanos en el ciberespacio haya sido una retardada tarea en el contexto global, lo cierto es que la *explosión* por interconectar al país, se dio en el año 2000, a través del proyecto e-México, en el que se consideró que la revolución de la información y las comunicaciones tenga un carácter verdaderamente nacional y se reduzca la brecha digital entre los gobiernos, las empresas, los hogares y los individuos, con un alcance hasta el último rincón de nuestro país.

En esta tesitura, el Plan Nacional de Desarrollo 2001-2006 (Presidencia de la República, 2001) estableció que la utilización de computadoras ha posibilitado la modernización de las actividades educativas, comerciales, industriales y de servicios. Sin embargo, las oportunidades en su aprovechamiento son dispares, atendiendo a las edades, grados educativos y niveles de ingreso. La situación en el caso de la telemática es aún menos equitativa, por los contrastes existentes en las posibilidades de acceso a Internet.

En este sexenio se estableció el Programa de Desarrollo Informático 2001-2006 (INEGI, 2002, p. 5), a través del cual se impulsó el Sistema e-México, el cual estaba abocado a coadyuvar a la creación de una infraestructura de acceso a la red mundial de comunicaciones, que acercara a la gran mayoría de los mexicanos a la información electrónica.

En el sexenio 2006-2012 se reconoció que México era el único país de la OCDE que no contaba con una política pública en materia de informática orientada a fomentar la SI. Por tal motivo, la Asociación Mexicana de Internet (2011, p. 5) propuso una Agenda Digital Nacional con el objetivo de definirla e identificar las propuestas de políticas pública necesarias para impulsar la innovación y competitividad de México, a través del uso de las tecnologías de información y comunicaciones, incluyendo el Internet y la banda ancha.

Con posterioridad, esta propuesta fue retomada por el Gobierno de la República, a través de una estrategia de política pública denominada *AgendaDigital.mx* (SCT, 2012, p. 4), cuyo objetivo central era la articulación y coordinación de acciones que los actores públicos y privados deberían realizar para que el país pueda obtener el mayor beneficio de las TIC a favor del desarrollo, la productividad y la competitividad.

Teniendo a cuesta una dilatada asimilación del fenómeno informático, en el sexenio 2012-2018, se impulsó la reforma de los artículos 6, 7, 27, 28, 73, 78, 94 y 105 de la Constitución Política de los Estados Unidos Mexicanos, mejor conocida como reforma estructural en materia de telecomunicaciones, por la cual se reconoció el derecho fundamental de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet.

Este derecho fundamental supone un hito constitucional para catapultar a la sociedad mexicana a la sociedad de la información y el conocimiento, mediante el establecimiento de políticas de inclusión digital universal, en donde la radiodifusión y las telecomunicaciones, amén de ser servicios públicos de interés general, se declaran áreas de rectoría económica del Estado.

Hoy día, la política de inclusión digital se viene desarrollando a través del proyecto México conectado, el cual provee conectividad en los sitios y espacios públicos, tales como escuelas, centros de salud, bibliotecas, centros comunitarios o parques, en los ámbitos de gobierno federal, estatal y municipal.

A efecto de hacer materializar este "novísimo" derecho fundamental, se ha establecido una Estrategia Digital Nacional que plantea cinco objetivos y cinco habilitadores transversales.

Específicamente en el habilitador "Inclusión y Habilidades Digitales", se establecen una serie de iniciativas, entre las que destacan las necesarias para la seguridad digital; en ella se plantea desarrollar proyectos que generen habilidades para la prevención de conductas delictivas contra niñas, niños y adolescentes, entre otros, ciberbullying, sexting, pornografía infantil y actos de violencia, en coordinación con las dependencias e instituciones competentes.

En tanto que en el habilitador "Marco jurídico" se establece la necesidad de armonizar la legislación para propiciar legalidad, certeza, seguridad y confianza a los individuos, las empresas y el gobierno en el uso de las TIC; es decir, para establecer una gobernanza de las TIC, situación que invariablemente implica la revisión de la legislación penal específica de los delitos informáticos.

Desde la perspectiva de la experiencia internacional, estos ilícitos se investigan por unidades especializadas, como son el *Federal Bureau of Investigation* en los Estados Unidos de Norteamérica, la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú, el Grupo de Delitos Telemáticos de la Guardia Civil Española, entre otros.

En el caso de México, la Policía Federal cuenta con la Policía Cibernética, cuyos esfuerzos se concentran en realizar acciones preventivas en materia de delitos cometidos en Internet, así como a la prevención y atención de denuncias de delitos contra menores. Básicamente sus actividades se orientan a identificar y desarticular organizaciones criminales de pedófilos, bandas internacionales de prostitución, que utilizan sistemas informáticos como medio de promoción y sobre todo de reclutamiento; así como investigar el fraude cibernético, piratería de software, intrusión

a sistemas de cómputo, hackeo, venta de armas y drogas por Internet y el ciberterrorismo.[4]

En este tipo de actividades, destaca su participación en la denominada *Operación Azahar*. A través de la cual la Guardia Civil Española en colaboración con las policías de Argentina, Brasil, Chile, Venezuela, República Dominicana, Panamá, EE.UU., Francia, Reino Unido, Polonia, Lituania, Letonia, Estonia, Ucrania e Israel, logró la mayor actuación policial internacional coordinada contra la distribución de pornografía infantil a través de las redes *peer to peer*.

Además de la Policía Cibernética, entidades federativas como Baja California, Ciudad de México, Estado de México, Guerrero, Hidalgo, Jalisco, Michoacán de Ocampo, Nuevo León y Yucatán, cuentan con unidades similares.

Ante la proliferación de estas Unidades Especializadas adscritas a las Procuradurías o Fiscalías Generales de Justicia Estatales, la Policía Federal desarrolló en el 2014 un Modelo de Policía Cibernética, cuyo fin es atender la Política de Seguridad Nacional del Estado Mexicano, la cual tiene como una de sus acciones impulsar, mediante la realización de estudios e investigaciones, iniciativas de ley que den sustento a las actividades de inteligencia civil, militar y naval, para fortalecer la cuarta dimensión de operaciones de seguridad: ciberespacio y ciberseguridad.

En esta tesitura, el gobierno federal ha establecido su visión sobre la ciberseguridad en el documento Estrategia Nacional de Ciberseguridad (2017, p. 4), cuyo objetivo general es identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano.

La Estrategia Nacional de Ciberseguridad planteó que, en el 2030, México sea una nación resiliente ante los riesgos y amenazas en el ciberespacio que aprovecha con responsabilidad el potencial de las TIC para el desarrollo sostenible en un entorno confiable para todos.

La estrategia reconoció a través de su eje transversal Marco jurídico y autorregulación la necesidad de adecuar el marco jurídico con el objetivo específico de homologar y armonizar la legislación penal en materia de delitos informáticos, así como dotar a las instancias encargadas de la procuración de justicia de las herramientas necesarias para su adecuada persecución.

Sin el propósito de menospreciar la visión que tiene la Estrategia Nacional de Ciberseguridad, vale advertir que omitió la importantísima labor que desempeñan otros operadores jurídicos, como es el caso de los abogados, especialista en materia de TIC y las instancias encargadas de la administración de justicia, es decir, de los litigantes, peritos particulares y los jueces que intervengan en los casos en que se busque enjuiciar a los presuntos responsables, pues por una parte, serán quienes en primera instancia analizarán y dictaminaran sobre la autenticidad y validez de indicios y pruebas vinculadas a crímenes informáticos, y en segunda, los que habrán de juzgar sobre el bien jurídico protegido, y en su caso, imponer la sanción que conforme a la legislación penal corresponda.

[4] El término se ha empleado fundamentalmente para hacer referencia a la posibilidad de que sean atacados tanto los sistemas de información como las redes de datos o que estos sean utilizados por y para perpetrar actos terroristas. *Vid.* Secciones 223 y 224 de la Homeland Security Act of 2002.

LEGISLACIÓN SOBRE CIBERDELINCUENCIA EN MÉXICO

La informatización de la sociedad y los fenómenos ilícitos que se desarrollan en el ciberespacio, han demandado la actualización de los marcos legales a nivel mundial, ello con el fin de reconstruir las hipótesis jurídicas existentes o construir nuevas categorías de conductas criminales frente al uso de la informática. Indudablemente, el ordenamiento jurídico mexicano no ha sido excepción.

En este contexto, nos referiremos, al sistema de regulación jurídica, que en su contenido y aplicación imbrica los principios y postulados del derecho penal al uso ilícito de la informática y las TIC, con el propósito es brindar seguridad jurídica a los usuarios, entidades y organizaciones respecto de distintos bienes jurídicos informáticos.

La *Convention on Cybercrime* estima que la lucha contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal, por lo que prevé diversas medidas que a nivel nacional deben adoptarse para hacer frente a esta fenomenología de cuello blanco, entre ellas la adecuación del marco jurídico para considerar los siguientes cuatro tipos de infracciones.

En primer lugar, establece las infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, mismas que se efectúan a través del acceso ilícito, la interceptación ilícita, ataques a la integridad de los datos y la integridad del sistema; pero también por el abuso de los dispositivos equipos e instrumentos técnicos.

En un segundo apartado se prevén a la falsificación y el fraude informático como Delitos Informáticos. En el tercero se establecen los delitos relacionados con el contenido, es decir, las conductas relativas a la pornografía infantil. Finalmente, establece las infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines.

En el caso específico de México, el acceso no autorizado e ilícito a equipos y sistemas de informática, interceptación ilícita, atentados contra la integridad de los datos y atentados contra la integridad del sistema se encuentran regulados en los artículos 180 y 181 fracción I del Código Penal para el Estado de Aguascalientes; 175 Ter, 175 Quáter y 175 Quinquies del Código Penal para el Estado de Baja California; 356 fracción V y 364 fracción I del Código Penal para el Estado de Baja California Sur; 405 fracción V, 440 y 442 del Código Penal para el Estado de Chiapas; 327 Bis del Código Penal para el Estado de Chihuahua; 336 fracción V del Código Penal para el Distrito Federal (Ciudad de México); 281 Bis fracciones I y II, 281 Bis 1 y 281 Bis 2 fracción I del Código Penal para el Estado de Coahuila; 201 fracción V del Código Penal para el Estado de Colima; 175 Bis fracción I y 400 fracción IV del Código Penal para el Estado de Durango; 174 fracción V del Código Penal para el Estado de México; 231 fracción II del Código Penal para el Estado de Guanajuato; 238 fracción XI y 344 fracción V del Código Penal para el Estado de Guerrero; 265 Bis fracción V del Código Penal para el Estado de Hidalgo; 143 Ter, 143 Quáter fracción I y 170 Bis fracción III del Código Penal para el Estado de Jalisco; 296 fracción V del Código Penal para el Estado de Michoacán; 148 Quáter fracción I y 189 Bis fracción I del Código Penal para el Estado de Morelos; 412 párrafo primero del Código Penal para el Estado de Nayarit; 225 Bis 2, 226, 241 Bis fracción V, 395

fracción X y 427 del Código Penal para el Estado de Nuevo León; 245 Bis fracción V del Código Penal para el Estado de Puebla; 159 Ter párrafo primero, 159 Quáter párrafo primero y 232 Bis fracción III del Código Penal para el Estado de Querétaro; 189 Bis fracción IV del Código Penal para el Estado de Quintana Roo; 231 último párrafo del Código Penal para el Estado de San Luis Potosí; 177 Bis A, 217 fracción I y 271 Bis fracción IV del Código Penal para el Estado de Sinaloa; 326 Bis del Código Penal para el Estado de Tabasco; 207 Quáter y 400 fracción V del Código Penal para el Estado de Tamaulipas; 314 fracciones I y II, 316 fracción I y 397 fracción V del Código Penal para el Estado de Tlaxcala; 181 fracción I del Código Penal para el Estado de Veracruz; 165 Sexies fracción I y 284 Bis fracción V del Código Penal para el Estado de Yucatán; 192 Bis del Código Penal para el Estado de Zacatecas; y, 211 Bis 1, párrafo segundo, 211 Bis 2, párrafo tercero, 211 bis 3, párrafos segundo y tercero, 211 bis 4 párrafo segundo y 211 bis 5 párrafo segundo del Código Penal Federal.

Entre las conductas ilícitas que encuadran en esta descripción, se encuentra el *Hacking*, la cual se caracteriza por el acceso no autorizado a un equipo o sistema informático. En el debate que representa la tipificación de los denominados Delitos Informáticos y en particular del *hacking*, se ha llegado a señalar la existencia de un tipo penal de acceso no autorizado simple y otro agravado, es decir, la conducta se agrava si tiene por objeto la producción de daños, que la intrusión tenga un fin específico, que a consecuencia de ello se tenga un resultado específico y, que la conducta tenga por objeto la violación de derechos intelectuales (Cámpoli, 2004, pp. 29-35) (Cámpoli, 2003, pp. 33-42) (Morón Lerma, 2000, p. 36) (Palazzi, 2000, pp. 85 y ss.).

De igual forma, la instalación de *sniffers o rastreadores* encajan en esta tipología, ya que suelen ser usados para penetrar en el disco duro de los ordenadores conectados a la red, buscando cierto tipo de información (Morón Lerma, 2000, p. 85).

En cuanto a las conductas relativas al abuso de equipos e instrumentos técnicos, se ubican conductas como los *Evil twins* y el *spyware*, o programas espía que se instalan en las computadoras personales para conocer los hábitos y actividades de familiares o empleados.

Estos ilícitos se encuentran regulados en diferentes términos y modalidades en los artículos 181 fracción II, 180 y 190 fracción XIV del Código Penal para el Estado de Aguascalientes; 175 Bis y 175 Quinquies del Código Penal para el Estado de Baja California; 338 del Código Penal para el Estado de Baja California Sur; 281 Bis y 281 Bis 2 del Código Penal para el Estado de Coahuila; 201 fracciones VI y VII, 234 fracción V y 290 fracción III del Código Penal para el Estado de Colima; 284 Bis inciso c), 326, 327, 327 Bis y 327 Ter del Código Penal para el Estado de Chihuahua; 439 párrafos primero y segundo, 440 y 441 del Código Penal para el Estado de Chiapas; 327 Bis del Código Penal para el Estado de Chihuahua; 336 fracciones IV y VI y 355 del Código Penal para el Distrito Federal (Ciudad de México); 175 Bis fracción I y 400 fracciones VI y VII del Código Penal para el Estado de Durango; 231 fracción I y V, y 234-A fracciones I, III, IV y VI del Código Penal para el Estado de Guanajuato; 344 del Código Penal para el Estado de Guerrero; 265 Bis del Código Penal para el Estado de Hidalgo; 143 Bis, 143 Ter, 143 Quáter fracción I, 170 bis del Código Penal para el Estado de Jalisco; 174 fracciones IV y VI del Código Penal para el Estado de México; 148 Quáter fracción I y 189 Bis fracción I del Código Penal para el Estado de Morelos; 296 del Código Penal para el Estado

de Michoacán; 412 párrafo segundo del Código Penal para el Estado de Nayarit; 178 fracciones I y II, 242 bis, 428 y 429 del Código Penal para el Estado de Nuevo León; 165 Ter fracción II del Código Penal para el Estado de Oaxaca; 477 y 478 del Código Penal para el Estado de Puebla; 159 Bis y 232 Bis del Código Penal para el Estado de Querétaro; 189 bis del Código Penal para el Estado de Quintana Roo; 217 fracción II del Código Penal para el Estado de Sinaloa; 326 Bis del Código Penal para el Estado de Tabasco; 207 bis, 207 Ter, 207 Quater, 207 Quinquies, 207 Sexies y 400 fracción IV del Código Penal para el Estado de Tamaulipas; 181 fracción I del Código Penal para el Estado de Veracruz; 243 Bis 2 fracción I del Código Penal para el Estado de Yucatán; 167 fracción VI, 168 Bis fracción I, 211 Bis, 211 Bis 1, 211 Bis 2, 254 Bis 1, 424 y 426 fracción II del Código Penal Federal; 112 bis y 113 bis 2 inciso b) de la Ley de Instituciones de Crédito; y, 376 fracciones IV y V de la Ley del Mercado de Valores.

Otras infracciones informáticas previstas en la Convención de Budapest son la falsificación y la estafa informática.

La primera se constituye como una conducta ilícita que tiene por objeto la indebida modificación, alteración o imitación de los originales de cualquier dato, archivo o elemento intangible contenido en sistema de redes de computadoras, base de datos, soporte lógico o programas; además, se combate la utilización o el aprovechamiento en cualquier forma de los bienes informáticos falsificados con conocimiento de esta circunstancia.

En este hecho delictivo encuadra el *Pharming*, y se presenta cuando un criminal informático desvía a un consumidor hacía una página electrónica apócrifa, aún y cuando el usuario haya escrito correctamente la dirección electrónica de la empresa con que desea contactar.

Así mismo, el *Phishing* constituye una conducta a través de la cual, mediante el envío de correos electrónicos o direccionamiento portales de Internet falsos, que en apariencia son enviados por instituciones con las cuales una persona tiene contacto, *v. gr.* un banco, pero dichos mensajes son disfrazados por redes bien organizadas de delincuentes informáticos que se hacen pasar por la institución con la que se está acreditado, y en el cual piden al usuario que actualice sus datos. Sin embargo, el usuario no estará actualizando sus datos, sino más bien proporcionándoselos a la delincuencia informática.

Este delito se encuentra previsto en los artículos 161 del Código Penal para el Estado de Aguascalientes; 259 del Código Penal para el Estado de Baja California; 335 y 356 del Código Penal para el Estado de Baja California Sur; 240 fracción IX del Código Penal para el Estado de Campeche; 405 del Código Penal para el Estado de Chiapas; 255 del Código Penal para el Estado de Colima; 400 fracciones I y II del Código Penal para el Estado de Durango; 167, 168 fracciones II, III, V y XI, 170 y 174 fracciones I y VI del Código Penal para el Estado de México; 234-a fracción II del Código Penal para el Estado de Guanajuato; 344 fracción VIII del Código Penal para el Estado de Guerrero; 265 Bis fracción I del Código Penal para el Estado de Hidalgo; 170 bis fracción I del Código Penal para el Estado de Jalisco; 296 fracciones I y VIII del Código Penal para el Estado de Michoacán; 220 Bis del Código Penal para el Estado de Morelos; 242 Bis fracciones I, II, III y IV del Código Penal para el Estado de Nuevo León; 245 Bis fracciones I, II, III y IV del Código Penal para el Estado de Puebla y 232 Bis fracción I del Código Penal para el Estado de Querétaro.

Por su parte, la estafa informática se caracteriza por la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de: la

introducción, alteración, borrado o supresión de datos informáticos; o, cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero.

En esta tipología, encuadra el *Spamming*. De acuerdo al reporte de legislación anti-spam elaborado por el *Task Force on Spam* de la OCDE (2006), tiene como objetivo conocer la naturaleza y facultades que tienen las autoridades gubernamentales, respecto a la imposición de las leyes aplicables al envió de información electrónica no solicitada.

El *Task Force on Spam* tiende a constituirse en una base que permita considerar a los países miembros de la OCDE, cómo es posible mejorar la capacidad de las agencias gubernamentales, frente a las quejas de los usuarios por el spam y cómo lograr la cooperación conjunta con terceros países.

En el reporte se da cuenta de que 19 países miembros de la OCDE, han adecuado su marco jurídico o bien han adoptado leyes específicas para la regulación del spam. Ahí mismo, se da cuenta de que tres países miembros se encuentran pendientes de emitir su legislación al respecto. Cinco Estados miembros usan las reglas y principios legales previamente existentes, para combatir la amplia gama de conductas criminales que se realizan a través de los servicios de correo electrónico, SMS, mensajes electrónicos instantáneos, fax, voz IP.

Reconoce que el spam es un problema de carácter internacional y que sólo mediante el establecimiento de políticas y legislaciones transfronteras será posible contar con las herramientas legales necesarias que permitan un combate exitoso a nivel mundial.

El reporte indica que las conductas realizadas por los *spammers* violan leyes sobre la protección al consumidor, leyes penales, leyes de protección de datos personales y leyes de telecomunicaciones.

Concluye que, en las leyes de los Estados miembros, se concentra el espíritu de las leyes anti-spam.

En el contexto de la legislación penal de las entidades federativas, la estafa informática se prevé en los artículos 241 fracción X del Código Penal para el Estado de Baja California Sur; 304 fracción XXIV del Código Penal para el Estado de Chiapas; 231 fracción XIV del Código Penal para el Distrito Federal (Ciudad de México); 211 fracción XXII del Código Penal para el Estado de Durango; 181 fracción I y 217 del Código Penal para el Estado de Veracruz; 226 Bis del Código Penal para el Estado de Chihuahua; 201 fracciones III y IV del Código Penal para el Estado de Colima; 400 fracción III del Código Penal para el Estado de Durango; 238 fracción XI del Código Penal para el Estado de Guerrero; 265 Bis fracción IV del Código Penal para el Estado de Hidalgo; 174 fracciones II y III del Código Penal para el Estado de México; 245 Bis párrafo segundo del Código Penal para el Estado de Puebla; y, 217 fracción I del Código Penal para el Estado de Sinaloa.

Como se apuntó líneas arriba, la Convención de Budapest contiene una tercera categoría de ilícitos, relativas a ciertos contenidos identificados como pornografía infantil, consistentes en su producción con la intención de difundirla a través de un sistema informático; su ofrecimiento o la puesta a disposición a través de un sistema informático; su difusión o transmisión a través de un sistema informático; procurarse o procurarla a otro a través de un sistema informático; o su posesión en un sistema informático o en un medio de almacenamiento de datos informáticos.

Este reprochable delito que atenta contra la infancia y la niñez, se encuentra regulado en los artículos 1 Código Penal para el Estado de Aguascalientes; 262 del Código Penal para el Estado de Baja California; 173 fracción I y II del Código Penal para el Estado de Baja California Sur; 170, 171 y 172 del Código Penal para el Estado de Colima; 333 del Código Penal para el Estado de Chiapas; 187 y 188 del Código Penal para el Distrito Federal (Ciudad de México); 170, 171 y 172 del Código Penal para el Estado de Colima; 236 del Código Penal para el Estado de Guanajuato; 173 del Código Penal para el Estado de Guerrero; 142-D y 142-H del Código Penal para el Estado de Jalisco; 204 fracción III y 206 del Código Penal para el Estado de México; 158 y 159 del Código Penal para el Estado de Michoacán; 212 del Código Penal para el Estado de Morelos; 201 Bis del Código Penal para el Estado de Nuevo León; 195 del Código Penal para el Estado de Oaxaca; 220 y 222 del Código Penal para el Estado de Puebla; 192 Bis del Código Penal para el Estado de Quintana Roo; 194 bis fracciones I, II, III, IV y V del Código Penal para el Estado de Tamaulipas; 211 del Código Penal para el Estado de Yucatán; 183 bis fracciones I y II del Código Penal para el Estado de Zacatecas; y, 200 párrafo primero, 202, 202 bis y 203 párrafo primero del Código Penal Federal.

Finalmente, concluye la Convención con las infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines, es decir, la lucha contra la fabricación y venta no autorizada de contenidos protegidos por los derechos de autor o los derechos conexos, se resume en el combate frontal a la piratería, lo cual incluye la lucha contra la imitación de productos originales.

En esta conducta se ubica el C*racking*. A diferencia del *hacker*, el *cracker* desconoce los sistemas informáticos y sus retos se limitan a la vulneración del software comercial acometiendo conductas de piratería informática (Morón Lerma, 2000, p. 32).

Al ser una materia de competencia federal, estas infracciones se encuentran previstas y sancionadas en los artículos 424 bis fracciones I y II, 426 fracción II y 429 del Código Penal Federal.

Finalmente, observamos que la actualización del marco jurídico no solamente se ha generado a través del proceso legislativo, pues la justicia constitucional ha desarrollado pautas interpretativas que orientan la interpretación de la ley frente al fenómeno que venimos tratando.

Al respecto, la Suprema Corte de Justicia de la Nación ha establecido el *principio de restricción mínima posible*, consistente en el deber del Estado para tomar todas las medidas necesarias para fomentar la independencia de las nuevas tecnologías de la información y la comunicación, en especial de Internet, para el intercambio de ideas y opiniones, y asegurar a los particulares su acceso.

Partiendo del derecho internacional de los derechos humanos, reconoce que, en el orden jurídico nacional, existe el principio relativo a que el flujo de información por Internet debe restringirse lo mínimo posible, esto es, en circunstancias excepcionales y limitadas, previstas en la ley, para proteger otros derechos humanos, como es la libertad de expresión y opinión.

Sin embargo, este criterio orientador contenido en la tesis aislada de jurisprudencia 2a. CII/2017 (10a.), no es del todo absoluto, ya que en la diversa tesis asilada 2a. CIV/2017 (10a.), el máximo tribunal mexicano estableció que el *principio de restricción mínima posible*, cuyo parámetro de regularidad es el no bloqueo excesivo de las páginas de Internet y el fomento de la libertad informática en el ciberespacio para el ejercicio adecuado de los derechos humanos, encuentra limite cuando las

opiniones o expresiones sean prohibidas, es decir, cuando devengan en un delito, tales como la incitación al terrorismo; 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–; la instigación directa y pública a cometer genocidio; la pornografía infantil o cuando la totalidad de los contenidos de una página web resulte ilegal.

Es posible que al amparo de las libertades de expresión y opinión se difundan ciertos contenidos ilícitos o presuntamente delictivos en Internet, circunstancia que obliga al establecimiento de parámetros penales e informáticos para su bloqueo o censura, situación que tanto la política como la legislación informática pasan por alto. Sin embargo, los ejercicios legislativos actuales en México distan mucho de equilibrar el establecimiento de una Estrategia Nacional de Ciberseguridad en la que se promueva la libertad de expresión en las relaciones sociales en masa por medios tecnológicos y la necesaria prevención derivada por su mal uso.

CONCLUSIONES

La *Convention on Cybercrime* constituye un marco de referencia global para el establecimiento de un marco jurídico estandarizado y homologado en materia de Delitos Informáticos.

En el caso de México –que aún continúa analizando su adhesión a la Convención de Budapest– el marco jurídico aplicable a los Delitos Informáticos, aunque si bien presenta avances significativos, lo cierto es que los códigos penales de las entidades federativas y los ordenamientos que en el ámbito federal contienen disposiciones relativas a estos ilícitos, contienen complejidades epistemológicas y hermenéuticas interpretativas.

Arribamos a esta conclusión, como resultado de un profuso análisis de la sintáctica, la semántica y la pragmática legislativa empleada para su tipificación y penalización.

Apartados de la singularidad política que conlleva el discurso del legislador ante cada creación normativa, atribuimos las complicaciones epistemológicas y hermenéuticas al desconocimiento del referente internacionalista que orienta la toma de decisiones en materia de Delitos Informáticos, pues *v. gr.* ilícitos como el acceso no autorizado a equipos y sistemas informáticos se considera como robo calificado (Aguascalientes).

Es de reconocer que las preocupaciones de los legisladores han gravitado en dar respuesta a ciertos reclamos sociales ante la comisión de delitos en los que la informática es un objeto o un instrumento para su comisión, tal es el caso del *sexting*, que es considerado como un delito contra la intimidad y la imagen (Baja California) o bien, como un delito de ultrajes a la moral o a las buenas costumbres e incitación a la prostitución (Jalisco). En otros casos, se observa que la producción legislativa se ha orientado hacia conductas lacerantes como la extorsión informática y telefónica como agravante (Aguascalientes, Baja California, Campeche, Chiapas, Ciudad de México, Colima, Durango, Estado de México, Nayarit, Oaxaca y Querétaro), el chantaje informático (Nuevo León), el secuestro cuando para su

comisión se empleen redes, sistemas informáticos o cualquier otro medio de alta tecnología, que facilite la consecución de los propósitos del secuestrador (Coahuila, Jalisco y Querétaro), o en sus modalidades equiparada (Baja California) y exprés (Oaxaca); el terrorismo (Baja California y Morelos), el uso indebido de información sobre actividades de las instituciones de seguridad pública, de procuración e impartición de justicia, así como las del sistema penitenciario (Colima y Estado de México), entre otros.

No proponemos la adecuación de la normativa penal a través de un tipo específico, es decir, la rotulación de un capítulo denominado Delitos Informáticos –varios códigos penales nacionales lo prevén en ese sentido–, ni insistimos en la necesaria homogeneidad en el establecimiento de sanciones privativas de libertad, en los requisitos de procedibilidad para su persecución, en la uniformidad para tipificarlos como delito grave o la impostergable tarea de prevenirlos mediante la educación y la generación de una cultura informática. Nuestra propuesta no es legislativa ni política, consiste en llamar la atención sobre la existencia de una hermenéutica penal que no conduzca a errores en la persecución de la criminalidad informática o la estigmatización de los ciberciudadanos, de ello dependerá en gran medida su enjuiciamiento y sanción, el desarrollo de la SI orientada a la competitividad económica, social y cultural de los mexicanos, así como al cumplimiento de los objetivos y el alcance de las metas establecidas en los instrumentos de planeación estratégica, lo cuales, en una visión de conjunto deberán actuar en el marco constitucional de promoción, respeto, protección y garantía de los Derechos Humanos y el necesario equilibrio entre informatización de la sociedad con los valores del Estado constitucional.

Bajo este marco, es imprescindible generar entre los ciudadanos una cultura de civilidad digital, es decir, de uso y aprovechamiento racional, ético, responsable e informado de las TIC, a efecto de que no solamente conozcan los riesgos de la informatización de la sociedad y las consecuencias de los ilícitos en la red, a la vez, deberá influirse positivamente para que coadyuven en la gobernanza de la red.

Finalmente, concluimos que México tiene ante sí un reto de gran envergadura en el cumplimiento de un deber global para garantizar la ciberseguridad de los ciudadanos y de las instalaciones estratégicas del desarrollo nacional, así como las de carácter económico, financiero, policial, militar y naval, de ahí la importancia de una correcta epistemología y hermenéutica penal informática que permita una paulatina adecuación del marco jurídico para adherirse a la Convención de Budapest sobre ciberdelincuencia, pues las guerras del futuro y el choque de civilizaciones en esos sectores se disputan hoy en el ciberespacio.

REFERENCIAS

1. A.A. V.V. (1999). Derechos Humanos: La condición humana en la sociedad tecnológica. En González R. Arnaiz, Graciano (coord.). *Derechos humanos y discurso político, Derechos Humanos: La condición humana en la sociedad tecnológica.* Madrid: Tecnos.

2. Amnesty International Ltd. (2018). Informe 2017/18, London.

3. Asociación Mexicana de Internet *et al.* (2011). *Agenda Digital Nacional*, *ADN*, México.

4. Bodenheimer, E. (1994). *Teoría del Derecho. México:* Fondo de Cultura Económica.

5. Bustamante, J. (1999). Derechos Humanos en el ciberespacio, en González R. Arnaiz, Graciano (coord.), *Derechos Humanos: La condición humana en la sociedad tecnológica*. Madrid: Tecnos, pp. 164-182.

6. Cámpoli, G. A. (2003). *Derecho Penal Informático*. San José, Costa Rica: Editorial Investigaciones Jurídicas.

7. Cámpoli, G. A. (2004). *Principios de Derecho penal Informático*. México: Ángel Editor.

8. Carrascosa, J. L. (2003). *Información: de la Sociedad de la Información a la Sociedad del Conocimiento*. Madrid: Ediciones Arcadia.

9. CNN (2017). *Xi Jinping pide 'soberanía cibernética' para regular internet según su conveniencia*, Internet. Recuperado de http://cnnespanol.cnn.com/2015/12/16/xi-jinping-pide-soberania-cibernetica-para-regular-internet-segun-su-conveniencia/#0.

10. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (2015). I*nforme de la Reunión de Expertos sobre Ciberlegislación y Regulación para Promover el Comercio Electrónico con Estudios de Casos y Análisis de Experiencias*, Ginebra.

11. Consejo de Europa (2001). *Convención sobre Ciberdelincuencia*. Budapest.

12. Consejo de Europa (2007). *Convenio para la protección de los niños contra la explotación y el abuso sexual*. Lanzarote.

13. Consejo de Europa (2003). *Protocolo relativo a la penalización de actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos*. Estrasburgo.

14. Consejo Nacional de Seguridad Pública (2016). Acuerdo 12/XL/16, México, Internet. Recuperado de http://dof.gob.mx/nota_detalle.php?codigo=5452136&fecha=09/09/2016.

15. Consejo Nacional de Seguridad Pública (2016). Acuerdo 06/XLI/16, México, Internet. Recuperado de http://www.dof.gob.mx/nota_detalle.php?codigo=5468583&fecha=04/01/2017.

16. Davara Rodríguez, M. Á. (1993). *Derecho Informático*. Pamplona: ARANZADI.

17. Departament of Homeland Security. *Homeland Security Act of 2002*.

18. Diario Oficial de la Unión Europea (2005). *Decisión Marco 2005/222/JAI*, Bruselas.

19. Eco, U. (2016). *De la estupidez a la locura. Crónicas para el futuro que nos espera*. México: LUMEN.

20. Estrategia Nacional de Ciberseguridad (2017). México. Recuperado de https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad.

21. Federal Bureau of Investigation. White-Collar Crime, Internet, 2017. Recuperado de https://www.fbi.gov/investigate/white-collar-crime.

22. Fix, F. H. (1990). *Informática y documentación Jurídica*. México: UNAM.

23. Friedman, Lawrence M. (1993). *Hacia una sociología jurídica de los noventas. Crítica Jurídica. Revista Latinoamericana de Política, Filosofía y Derecho*, (12). Instituto de Investigaciones Jurídicas-UNAM, México, pp. 55-57.

24. García Máynez, E. (1999). *Positivismo Jurídico, Realismo Sociológico e Iusnaturalismo*. México: Fontamara.

25. Goodman, M. (2003). *Cibercriminalidad*. México: INACIPE.

26. González R. Arnaiz, G. (1999) (coord.). *Derechos humanos y discurso político, Derechos Humanos: La condición humana en la sociedad tecnológica*. Madrid: Tecnos.

27. Gordon, Graham (2001). *Internet: Una indagación filosófica*. Madrid: Ediciones Cátedra.

28. Instituto Nacional de Estadística, Geografía e Informática (INEGI) (2002). *Programa de Desarrollo Informático 2001-2006*, México: INEGI.

29. Instituto Nacional Electoral (INE) (2017). Conoce el convenio de colaboración firmado entre el INE y Facebook, México. Recuperado de http://centralelectoral.ine.mx/2018/02/13/conoce-el-convenio-de-colaboracion-firmado-entre-el-ine-y-facebook/.

30. Moles Plaza, R. J. (2004). *Derecho y Control de Internet. La regulabilidad de Internet*. Barcelona: Ariel.

31. Morón Lerma, E. (1999). *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red*. Pamplona: ARANZADI.

32. Nora, S. y Minc, A. (1980). *La Informatización de la sociedad*. México: Fondo de Cultura Económica.

33. OECD (1984). *Computer related criminality: analysis of legal policy in the OECD Area*, ICCP.

34. OECD (2006). *Report of the OECD task force on spam: anti-spam toolkit of recommended policies and measures*.

35. Palazzi, P. A. (2000). *Delitos Informáticos*. Buenos Aires: Ad-Hoc.

36. Parent Jacquemin, J. (1986). *Eros y Ethos Informáticos*. México: UAEM.

37. Parisier, E. (2017). *El Filtro burbuja*. México: Taurus.

38. Pérez Luño, A. E. (2004). *¿Ciberciudadaní@ o ciudadanía.com?* Barcelona: Gedisa.

39. Pérez Luño, A. E. (1987). *Nuevas tecnologías, sociedad y derecho: El impacto socio-jurídico de las N.T. de la información*. Madrid: Fundesco.

40. Piña Libién, H. R. (2008). *El derecho a la autodeterminación informativa y su garantía en el ordenamiento jurídico mexicano*. México: Infoem. Recuperado de: https://www.infoem.org.mx/doc/publicaciones/2008/PET_2006.pdf.

41. Postman, N. (1994). *Tecnópolis: la rendición de la cultura a la tecnología*. Barcelona: Círculo de Lectores.

42. Presidencia de la República (2001). *Plan Nacional de Desarrollo 2001-2006*, México. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/89909/PlanNacionaldeDesarrollo2000-2006.pdf.

43. Presidencia de la República (2013). *Plan Nacional de Desarrollo 2013-2018*. México. Recuperado de http://pnd.gob.mx/.

44. Presidencia de la República (2014). *Programa Nacional de Seguridad Pública 2014-2018*. México. Recuperado de http://www.dof.gob.mx/nota_detalle.php?codigo=5343081&fecha=30/04/2014.

45. Presidencia de la República (2014). *Programa para la Seguridad Nacional 2014-2018. México*. Recuperado de http://www.presidencia.gob.mx/wp-content/uploads/2014/05/Programa-para-la-Seguridad-Nacional-Versio%CC%81n-Final.pdf.

46. Presidencia de la República (2013). *Programa para un Gobierno Cercano y Moderno 2013-2018*. México. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/3114/programa-para-un-gobierno-cercano-y-moderno.pdf.

47. Roszak, T. (1990). *El culto a la información*. México: Grijalbo-CONACULTA.

48. Secretaría de Comunicaciones y Transportes (SCT) (2012). *AgendaDigital.mx*, México: SCT.

49. Wark, J. (2011). *Manifiesto de Derechos Humanos*. España: Baratalia.

50. Zavala Alardín, G. (1990). *La Sociedad Informatizada ¿Una nueva utopía?* México: Trillas.