Una aproximación al Ciberderecho

I. Introducción

El llamado Ciberderecho o Derecho de Internet debe entenderse a partir del ciberespacio, que Moisés Barrio Andrés define como:

> "el espacio global en el entorno de la Sociedad de la información que consiste en el conjunto interdependiente de infraestructuras de las Tecnologías de Información y Comunicación (TIC), y que incluye a Internet, las redes de telecomunicaciones, los sistemas informáticos y los procesadores y controladores integrados propios del Internet de las Cosas" [1].

Según el autor, el ciberespacio ha revolucionado la comunicación entre las personas, organizaciones, instituciones y gobiernos en un entorno virtual denominado *cibercosmópolis*, que ofrece enormes beneficios y ventajas, pero también vulnerabilidades y riesgos potenciales que por el anonimato de sus operadores, exponen a la comunidad cibernauta a delitos como el fraude cibernético, violaciones de propiedad intelectual, extorsión, *hacking*, pornografía, trata de personas, terrorismo, entre otros.[2]

Éste escenario virtual, ha llevado al operador jurídico a definir los campos de actuación electrónica que tendría que aplicar en cada disciplina del derecho, para poder estar en posibilidad de trasladar sus conceptos fundamentales, a la protección de la comunidad cibernauta.

Ante ello, se ha planteado cómo se deben proteger los derechos fundamentales y qué tratamiento deben tener los acuerdos de voluntades o contratos, los delitos, la seguridad nacional, entre otros, a través del uso del

[1] Moisés Barrio Andrés, *Ciberderecho, Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet*, Tirant lo Blanch, Valencia, 2018, p.25.

[2] *Ibidem,* p. 18.

medio electrónico, para determinar de inicio, un catálogo universal básico de "derechos digitales", y así estar en posibilidad de abarcar los mayores esquemas sociales de coordinación y subordinación que se generan en el ciberespacio.

II. Soberanía del ciberespacio

Para responder a los cuestionamientos planteados, es necesario analizar el ámbito de interacción y de competencia que requiere un espacio "autónomo" como el ciberespacio; ¿acaso su constante expansión requiere de una autorregulación que se encuentre libre de una soberanía estatal?, sobre todo si consideramos que no existe "territorio, población y gobierno"[3] digital delimitado para los Estados en este mundo intangible que no tiene fronteras.

Al respecto, Stefan A. Kayser, en su investigación *El ejercicio de la Soberanía de los Estados* reitera que al abordar el concepto de "soberanía" debe considerarse de manera indispensable, la existencia del elemento geográfico:

> "Solo dentro de la jurisdicción de su ámbito, principalmente en su territorio, los Estados pueden ejercer su soberanía. "Esta soberanía no puede ser ejercida fuera del territorio excepto en virtud de una norma que lo permita, derivada de la costumbre internacional o de un convenio". La aplicación geográfica de la soberanía juega un papel importante en ambas esferas, en la nacional y en la

[3] Recordemos que la teoría de los tres elementos del Estado, expresan los mínimos de un Estado para ejercer su soberanía. Stefan A. Kayser precisa que "La soberanía es uno de los principios cardinales de la teoría del Estado. La soberanía de los Estados denota el derecho legal inalienable, exclusivo y supremo de ejercer poder dentro del área de su poder. (…) La soberanía está arraigada en el concepto de Estado. Sólo el estado tiene soberanía. Sólo el Estado –a través de sus órganos- puede ejercer los derechos legales y la autoridad de los poderes del Estado. Ninguna persona, ni física ni moral, puede asumir tales derechos soberanos, a menos que sean órganos del Estado y actúen con la capacidad de uno de sus órganos." Stefan A. Kayser, *El ejercicio de la soberanía de los estados*, Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM, México, p.85. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/6/2790/6.pdf

> internacional. Nacionalmente el territorio del Estado limita el área de jurisdicción. Internacionalmente, el territorio del Estado define las fronteras entre Estados iguales."[4]

En consideración de esta precisión habría que afirmar la existencia de la jurisdicción de un Estado en el ciberespacio con base a criterios de territorialidad, es decir, su jurisdicción soberana comprendería tanto las actividades virtuales realizadas en su territorio, como la infraestructura física, soportes técnicos, cables, líneas nacionales y páginas *web* que se encuentren alojadas dentro de las fronteras de un país.

También es importante revisar los compromisos internacionales específicos que cada Estado tenga suscritos cuando se trate de actividades virtuales que nacionales realicen en el extranjero. Países de la Unión Europea (UE), como España, Alemania o Suiza contemplan criterios de jurisdicción por nacionalidad, en el que deben respetarse tanto el *principio de personalidad activa* como el *principio pro persona pasiva*[5], el primero para que un Estado puede ejercer jurisdicción sobre un nacional que cometió un ciberdelito en el extranjero; y el segundo, para proteger a las víctimas nacionales que han sufrido un hecho ilícito como el ciberterrorismo en un estado foráneo. Asimismo, encontramos dentro de la UE la adopción del *principio real o de protección* [6] ,que establece la intervención del Estado cuando se vea amenazada la seguridad nacional en el ciberespacio, ya sea bloqueando los sitios *web* de amenaza o limitando el acceso a ellos, con apoyo de organizaciones públicas y privadas que mencionaremos más adelante.

En virtud de lo anterior, al considerar los criterios de territorialidad y la nacionalidad para delimitar la soberanía de un Estado en el ciberespacio, se

---

[4] *Ibidem,* p. 92.

[5] Enrique Bacigalupo, *Derecho Penal. Parte General,* Ed. Hammurabi, 2ª edición, 1ª reimpresión, Buenos Aires, 2007, p. 182

[6] *Ibidem,* p.181.

puede determinar que el ciberespacio no puede ser soberano en sí mismo con una comunidad cibernética única, ajena y de autodeterminación, ya que representaría considerar a un "pueblo cibernético" de usuarios infinitos y que todos los Estados y organizaciones internacionales existentes renunciaran a su ejercicio potestativo en el mundo virtual, lo que significaría a su vez una separación del "mundo físico". En palabras de Moisés Barrio Andrés, "el ciberespacio no puede convertirse en soberano, pero sí está sujeto a la soberanía de los Estados"[7].

III. Garantía de los derechos en el ciberespacio

Una vez que hemos determinado que cada Estado debe regular su ámbito virtual, es importante abordar la problemática que las diferencias de contenido, desarrollo tecnológico e intereses de cada Estado, y sus actores no estatales, afectan para tener una regulación pública y de cooperación internacional equilibrada, sobre todo que salvaguarde los derechos fundamentales de las personas; por lo mismo, la pregunta no es si el ciberespacio puede regularse, más bien ¿cómo debe regularse y por quién?

Sabemos que el Internet surge en Estados Unidos "como un espacio de libertad sin limitaciones"[8], por lo que la resistencia de algunos cibernautas a que el Estado resolviera los conflictos de intereses era lógica por el temor a que éste restringiera arbitraria o indebidamente su acceso. No obstante, sin la debida regulación estatal, ¿cómo podría proclamarse un espacio de libertad sin protección de este derecho de libertad por la única autoridad reconocida para

[7] Moisés Barrio Andrés, *op. cit.,* p.37.

[8] A pesar de que en 1969, 1982 y 1983 se registran los primeros antecedentes de redes sin nodos centrales, es hasta 1990 que el británico Tim Berners-Lee lanza el Hyper Text Markup Language (lenguaje de marcas de hipertexto) conocido como HTML y la primera gran red mundial "World Wide Web". Para conocer más, se pone a disposición el artículo de Vicente Trigo Aranda, *Historia y Evolución de Internet*, publicado con Autores científicos-técnicos y académicos (ACTA):
https://www.acta.es/medios/articulos/comunicacion_e_informacion/033021.pdf

su protección? por ello, la aplicación de los principios propuestos por la doctrina, surgida del Derecho Comparado, en base a los modelos regulatorios conocidos[9], resulta fundamental en la labor jurisdiccional.

Por ello, haremos alusión a una serie de principios basados en la propuesta del doctrinario Moisés Barrio Andrés, como referencia del tratamiento pionero que la legislación europea ha realizado, al amparo de distintos instrumentos internacionales:

[9] Existen 4 modelos regulatorios, a saber: **1. *Modelo regulatorio que extiende la soberanía territorial del Estado al ciberespacio*.-** donde el ciberespacio observa las disposiciones vigentes de los ordenamientos jurídicos territoriales que pueden trasladar su ámbito de competencia al campo electrónico, como son las cuestiones fiscales, de propiedad intelectual, de protección de datos, de comercio electrónico y de protección al consumidor. Este modelo predomina por la facilidad de localizar geográficamente a los usuarios y los sitios de internet, pero se critica por regular excesivamente las actuaciones de los cibernautas, lo que provoca menos competencia e innovación. **2. *Modelo regulatorio con base de acuerdos internacionales que establezcan parcelas de regulación armonizadas*.-** el cual busca la celebración de convenios internacionales entre los Estados para determinar un marco jurídico básico para cada área del ciberespacio. En este modelo se ha regulado, "…en áreas como el cibercrimen o la transferencia internacional de datos. [sin embargo] Los Estados mantienen todavía un férrea resistencia a la incorporación de normas jurídicas generadas en el exterior". **3. *Modelo regulatorio que busca crear organismos internacionales que coadyuden a la regulación del ciberespacio*.-** A la fecha existen organismos como *Internet Corporation for Assigned Names and Numbers* (ICANN), el *World Wibe Web Consortium* (W3C) o la *Internet Society* (ISOC), que si bien son buenos esfuerzos para promover una sana interacción de los cibernautas, todavía no tienen mucho impacto. Para mejor referencia: El ICANN, conocida en español como la *Corporación para la Asignación de Nombres y Números en Internet* "es una corporación de beneficio público, sin fines de lucro, con participantes de todo el mundo dedicados a mantener una Internet segura, estable e interoperable. Promueve la competencia y desarrolla políticas relacionadas con los identificadores únicos de Internet. Mediante su rol de coordinador del sistema de nombres de Internet, tiene un impacto importante en la expansión y evolución de la misma." Para conocer más de la "ICANN" consulte: https://www.icann.org/resources/pages/what-2012-02-25-en; El "W3C" o en español, *El Consorcio World Wide Web* es una comunidad internacional dirigida por el inventor de la Web ya mencionado, Tim Berners-Lee, que trabaja conjuntamente para desarrollar estándares web y llevarla a su máximo potencial. https://www.w3.org/Consortium/; y el "ISOC" es una comunidad global que busca proporcionar una estructura organizativa del internet y garantizarla para todos de forma transparente y abierta: https://www.internetsociety.org/es/about-internet-society/ **4. *Modelo regulatorio de la arquitectura seminal del ciberespacio*.-** que "… aprovecha la particular arquitectura o "código" de la Red para producir efectos regulatorios: el ciberespacio se reglamenta no sólo en virtud de las técnicas clásicas de regulación de normas jurídicas, sino también, y sobre todo por su arquitectura estructural. [La crítica es que estos "códigos" son creados] por actores privados ancladas en sectores de una sociedad funcionalmente diferenciada de la física y no en los Estados."
Moisés Barrio Andrés, *op. cit.,* pp. 69 a 72.

1. **El Principio de libertad de expresión cibernética**.- Este principio se basa en el derecho humano a la libre manifestación de ideas, contenidos en el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP)[10]. Este derecho puede incluir, el acceso universal al ciberespacio sin discriminar a ningún usuario; y se recoge en el mal llamado *derecho fundamental de acceso al Internet*[11].

2. **Principio de neutralidad del ciberespacio y su neutralidad tecnológica**.- el cual busca preservar el carácter abierto de la red, cuyos límites estarían determinados por la licitud de contenidos que generen los proveedores de la red y donde la innovación tecnológica no establezca estándares que limiten la libre competencia. El antecedente lo recoge la Unión Europea con el *Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 por el que se establecen medidas en relación con el acceso a una internet abierta y se modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas y el Reglamento (UE) no 531/2012 relativo a la itinerancia en las redes públicas de*

[10] "**Artículo 19.-** 1. Nadie podrá ser molestado a causa de sus opiniones. 2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. 3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para: a) Asegurar el respeto a los derechos o a la reputación de los demás; b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas." Consulta en: https://aplicaciones.sre.gob.mx/tratados/ARCHIVOS/DERECHOS%20CIVILES%20Y%20POLITICOS.pdf

[11] Que según el autor de referencia está reconocido por el artículo 15.1.b del *Pacto Internacional de Derechos Económicos, Sociales y Culturales* (PIDESC), del 16 de diciembre de 1966, al prever el derecho de "gozar de los beneficios del progreso científico y de sus aplicaciones". Referencia en:
https://www.ohchr.org/SP/ProfessionalInterest/Pages/CESCR.aspx

comunicaciones móviles en la Unión (Texto pertinente a efectos del EEE)[12]

3. **Principio de buena fe**.- o las denominadas "políticas de privacidad", que obligan a los proveedores de servicio a informar a todo usuario de su servicio electrónico, de la tecnología a emplear en dicho servicio, así como el tratamiento de los datos que proporcione, principalmente de los datos personales. Si bien la Unión Europea fue pionero en la protección normativa, en México ya se reconoce la protección de los datos personales a nivel constitucional, federal y estatal[13].

4. **Principio de la privacidad**.- vinculada con el principio anterior, busca proteger la decisión del usuario de disponer su información hacia terceros en los términos que éste elija, para salvaguardar la confidencialidad, identidad, intimidad y secrecía de sus comunicaciones. El artículo 17 del *Pacto Internacional de Derechos Civiles y Políticos*, vigente desde 1976, establece la premisa de protección de la vida privada, de la cual deriva este principio[14].

---

[12] Este Reglamento tiene por objeto "(…)establecer normas comunes destinadas a garantizar un trato equitativo y no discriminatorio del tráfico en la prestación de servicios de acceso a internet y a salvaguardar los derechos de los usuarios finales. Su finalidad no es solo proteger a los usuarios finales, sino garantizar simultáneamente el funcionamiento continuado del ecosistema de internet como motor de innovación." Se recomienda su consulta en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32015R2120

[13] La *Constitución Política de los Estados Unidos Mexicanos*, en su artículo 16 salvaguarda el derecho que tiene toda persona a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley. De igual forma, la protección de datos personales en posesión del sector privado se regula por la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* y a nivel estatal, se encuentran las disposiciones locales de protección específicas vigentes.

Para ahondar más sobre el tema de protección de datos, se recomienda la lectura del ensayo *Derecho al Olvido Digital*, que el Centro de Ética Judicial publicó en la siguiente liga: https://www.centroeticajudicial.org/uploads/8/0/7/5/80750632/consideraciones_en_torno_al_derecho_al_olvido_digital.pdf

[14] El artículo 17 establece que "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y

5. **Principio de la cooperación jurídica internacional**.- que surge principalmente para investigar los ilícitos cometidos en el ciberespacio, generalmente por usuarios fuera de su jurisdicción, de tal forma que a través de la cooperación de las distintas jurisdicciones involucradas se coadyuve a la persecución de los ciberdelitos. La gran referencia de esta cooperación internacional la encontramos en el *Convenio sobre la ciberdelincuencia*, celebrado el 23 de noviembre de 2001 en Budapest por el Consejo Europeo[15].

6. **Principio de la seguridad desde el diseño**.- el cual exige sistemas de seguridad desde el desarrollo del diseño de una tecnología cibernética, para la protección y prevención de ilícitos por parte de terceros, de la información que se resguarde en dichos sistemas. Como expondremos en el siguiente apartado, nuestro país ya cuenta con estrategias nacionales que buscan implementar medidas de seguridad para evitar ataques cibernéticos.

Dicho lo anterior, analizaremos el caso en derecho comparado que resuelve sobre la libertad de expresión cibernética, a saber, el caso *JANET RENO, ATTORNEY GENERAL OF THE UNITED STATES, et al., APPELLANTS v. AMERICAN CIVIL LIBERTIES UNION et al.*[16], que surge cuando se demanda la inconstitucionalidad de algunas disposiciones del

---

reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques" Para mayor consulta: https://aplicaciones.sre.gob.mx/tratados/ARCHIVOS/DERECHOS%20CIVILES%20Y%20POLITICOS.pdf

[15] Este instrumento internacional es el primero en proponer una cooperación internacional entre Estados, para investigar y perseguir penalmente los ciberdelitos. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

[16] Sentencia completa disponible en: https://supreme.justia.com/cases/federal/us/521/844/.

Communications Decency Act [17] o "CDA", promulgada el 8 de febrero de 1996 en Estados Unidos de América (EUA), por vulnerar el derecho a la libertad de expresión que protege la Primera Enmienda; el CDA buscaba regular la verificación de identidad de las personas que hacen uso de Internet, estableciendo la prohibición y acción penal contra cualquiera que acosara o transmitiera contenidos obscenos e indecentes a personas menores de 18 años. Considerando que en ese entonces la tecnología no era suficiente para verificar la identidad ni edad del usuario, un juez de distrito resolvió dictar una medida cautelar temporal que suspendía la aplicación de los artículos impugnados. Tras el desahogo y confirmación de la suspensión en instancias subsecuentes por un Tribunal de Distrito, se buscó llevar el caso ante la Corte Suprema de Justicia de los EUA.

En junio de 1997, la Corte Suprema resolvió confirmar la sentencia del Tribunal de Distrito, por determinar que la CDA vulneraba la Primera Enmienda, argumentando que no existían en dicho momento los medios tecnológicos que dieran cumplimiento a la reglamentación prevista por dicho ordenamiento, especialmente para verificar la edad de los receptores del contenido "indecente", y al ser una ley penal, ponía en riesgo al Gobierno de aplicar sanciones sin certeza probatoria a adultos que pudieron no haber tenido intención de tener acceso a dicho contenido o que por el contrario, quisieran tener libre acceso al mismo sin restricciones.

Cabe señalar, que sí este caso fuera discutido en estos momentos, la valoración de los jueces respecto a los procesos electrónicos que verifican la identidad y edad de un participante en la Internet cambiaría radicalmente, por lo que debe tenerse mucho cuidado en la revisión de los elementos que se toman en cuenta para resolver un caso donde la tecnología define el curso a seguir.

[17] Traducción en español como *Ley de Decencia en las Comunicaciones,* de la cual se reclamaron principalmente dos artículos: artículo 223(a)(1) que vinculaba a los problemas que plantea la verificación de edad en el Internet, mientras que el artículo 223(d) prohibía la disponibilidad de contenido sexual explícito a personas menores de 18 años.

IV. México en el ciberespacio

En el caso de México, es incipiente el tratamiento del ciberespacio, por ello es urgente agilizar su implementación jurídica e institucional, de lo contrario, seguiremos observando una ciberseguridad nacional expuesta a constantes ataques cibernéticos.

Apenas en 2017, se estableció la *Estrategia Nacional de Ciberseguridad*[18]*(ENCS)*, con el objeto de "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." [19], misma que se fundamentó en tres Programas a) el *Plan Nacional de Desarrollo 2013-2018* y al logro de los objetivos del *Programa para un Gobierno Cercano y Moderno 2013-2018*, b) *Programa Nacional para la Seguridad Pública 2014-2018* y c) el *Programa para la Seguridad Nacional 2014-2018*, la cual corre a cargo de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE). Un primer reporte de la ENCS expuso la situación cibernética de nuestro país:

> "(…) En México, los internautas han pasado de 40 a 65.5 millones en tan solo 4 años (2012 a 2016). De acuerdo al reciente estudio Hábitos de los Internautas en México de la Asociación Mexicana de Internet MX, en México se han registrado hasta 70 millones de cibernautas en 2016. La Policía Federal, a través de la División Científica, impulsó una Estrategia de Ciberseguridad para fortalecer, entre otros, la concientización social sobre el uso responsable de las TIC. Además el número de incidentes cibernéticos identificados, se ha triplicado de 2013 a 2016, pasando de cerca de 20 mil incidentes a más de 60 mil; mientras que la presencia de sitios web apócrifos con fines de fraude, se incrementó un 11 por ciento

[18] Consultable en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

[19] *Ibidem,* p.4.

> entre 2015 y 2016, llegando a cerca de 5 mil; la propagación de virus informáticos con afectaciones en México creció un 57 por ciento de 2015 a 2016, llegando a cerca de 40 mil eventos, destaca el grado de sofisticación utilizado por los ciberdelincuentes en algunos de los casos. Por su parte, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) señala que: durante el primer trimestre del 2011, el fraude cibernético pasó del 7 por ciento (38 mil 539 quejas) de las reclamaciones por posible fraude, al 42 por ciento (639 mil 857 quejas) en el mismo periodo del 2017. El monto reclamado en el primer trimestre de 2017 asciende a mil 167 millones de pesos, del cual se abonó el 53 por ciento del total; y el 90 por ciento de los asuntos se resolvieron a favor del usuario. En cuanto al canal por donde más se presenta el fraude cibernético, el 91 por ciento es por comercio electrónico y llama la atención el incremento de las operaciones por internet para personas físicas y de banca móvil (167 por ciento y 74 por ciento respectivamente) en comparación al año anterior. Por su parte, en 2017, el promedio mensual de fraudes cibernéticos en comercio electrónico fue de 193 mil casos, cuando el año anterior era de solo 131 mil. En cuanto a fraudes cibernéticos en banca móvil, en el mes de marzo de 2017 se presentó una cifra histórica con 3 mil 682 casos (…)"[20]

El reporte transcrito evidencia que hace falta una adecuada fiscalización y regulación de este medio electrónico, el cibercrimen costará al mundo y a nuestro país[21] millones de dólares para su atención; tan solo recordemos como en el mes de abril del 2018, el Banco de México enfrentó uno de los más graves ataques cibernéticos en los último años, cuando el Sistema de Pagos Electrónicos Interbancarios fue *hackeado* para extraer dinero de cuentas de varias instituciones bancarias por más de 300 millones de pesos[22]; el Director del Banco de México (BANXICO), Alejandro Díaz de León Carrillo, anunció tras

[20] *Ibidem,* p.6.

[21] "(…) el cibercrimen le cuesta al mundo hasta US$575,000 2 millones al año, lo que representa 0.5 por ciento del producto interno bruto global. Eso es casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional. En América Latina y el Caribe, este tipo de delitos nos cuestan alrededor de US$90,000 millones al año. Con esos recursos podríamos cuadruplicar el número de investigadores científicos en nuestra región.(…)" *Ibidem,* pág. 5-6.

[22] La cronología del ataque cibernético a BANXICO puede consultarse en la nota periodística del 18 de mayo de 2018 del periódico Expansión, en el siguiente vínculo: https://expansion.mx/economia/2018/05/18/caso-spei-la-cronologia-del-hackeo-al-sistema-financiero-mexicano

este ataque la creación de una Dirección de Ciberseguridad, para fortalecer la seguridad de la información y por la cual ha perseguido activamente a las instituciones que no protegen a sus usuarios de los mismos[23].

Al respecto, el *Índice Mundial de Ciberseguridad 2018*, de la Unión Internacional de Telecomunicaciones (ITU), organismo dependiente de la Organización de las Naciones Unidas para abordar el tema, elabora desde el 2014 un estudio anual de sus 193 miembros, para definir los avances de la ciberseguridad en el mundo en sus aspectos de cooperación internacional, legales, técnicos, organizacionales, educacionales y de cultura sobre el tema, ubica al Reino Unido en primer lugar y a México en el lugar 63 con un nivel "medio" de seguridad, en el que su legislación en la materia se encuentra en proceso de maduración, desarrollo y actualización[24], lo que resulta preocupante si consideramos que en 2017 ocupaba el lugar 28.[25]

A su vez, la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo, a través del estudio realizado por el Observatorio de Ciberseguridad en América Latina y el Caribe denominado *Informe de*

[23] Destaca la nota periodística del periódico Expansión del 12 de junio de 2019, que reporta el inicio de proceso de sanción de BANXICO a 18 instituciones financieras que no han implementado medidas de protección en los pagos electrónicos interbancarios. Para mayor referencia léase en: https://expansion.mx/economia/2019/06/12/banxico-preve-sancionar-a-18-instituciones-tras-hackeo-via-spei

[24] Estadística de México disponible en la página 56 del Índice: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

[25] Viene a la memoria la nota periodística del 22 de mayo de 2019, por el periódico INBOBAE, que reporta cómo la Agencia de Investigación Criminal de la Fiscalía General de la República, después de una denuncia anónima logro incautar a una banda de hackers que mediante un software lograban entrar al Sistema de Pagos Electrónicos Interbancarios (SPEI) para hackear cajeros automáticos, con lo que lograron sustraer entre 200 y 400 millones de pesos. Lo anterior, pone en evidencia el surgimiento de diversas bandas de hackers que vinieron después del mayor golpe al sistema financiero mexicano y que representan un desafío en su rastreo por parte de las autoridades digitales. Para mayor lectura de la noticia: https://www.infobae.com/america/mexico/2019/05/22/como-atraparon-a-la-mayor-banda-de-hackers-mexicanos-que-orquesto-robos-millonarios-al-sistema-bancario/

Ciberseguridad 2016, ¿Estamos preparados en América Latina y el Caribe?[26], ubica también a México en un nivel intermedio de madurez de protección con diversas áreas de oportunidad de resolver en las cinco dimensiones de estudio: política, sociedad, educación, legislación y tecnología.

A nivel jurisdiccional, y desde el golpe al sistema financiero mexicano al que se ha hecho mención, se observa un incremento de casos que demandan el ataque por parte del *cibercrimen* anónimo, pero también estamos conociendo de diversos asuntos que se suscitan a consecuencia de la interacción entre usuarios del ciberespacio nacional.

Al respecto, resalta el criterio que la Segunda Sala de la Suprema Corte de Justicia de la Nación (SCJN), emitió derivado del amparo indirecto que se promovió contra el bloqueo a un periodista de la cuenta de *Twitter* del Fiscal General del estado de Veracruz en 2017. El periodista manifestó que el bloqueo de esta cuenta pública violaba su *derecho de acceso a información de carácter público y de interés general*, así como de su *derecho de libertad de expresión*, pues utiliza *Twitter* para difundir notas y mantener contacto con las autoridades del estado, por lo que debía considerarse también una limitación a su "herramienta de trabajo".

El Juez de Distrito amparó al quejoso para desbloquearlo de la cuenta del Fiscal, sentencia que fue recurrida por el Fiscal quien alegó violación al principio de agravio personal y directo, variación de la litis y violación a la confidencialidad de su información personal. Finalmente, la Segunda Sala de la SCJN resolvió el amparo en revisión 1005/2018[27], confirmando la sentencia recurrida por las razones siguientes[28]:

[26] Consultar más del reporte para México en la página 86 del Informe que se pone a disposición en: https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe

[27] Para mejor referencia del caso, puede consultarse el proyecto de sentencia público que se puso a disposición al amparo de los artículos 73 párrafo segundo y 184 párrafo primero de la

a) **"La cuenta de un servidor público debe ser de interés general para la sociedad"**, por referir actividades públicas que derivan del cumplimiento a su gestión pública.

b) **"La prevalencia del derecho a la información sobre el derecho a la intimidad debe ser proporcional y encontrarse justificada"**, lo cual no ocurrió en el caso por el hecho de que el Fiscal voluntariamente se sometió al escrutinio público al difundir información por este medio digital.

c) **"La publicidad de la cuenta Twitter del Fiscal está justificada",** ya que el Fiscal General al momento de crear su cuenta, la hizo pública, cuando tenía oportunidad de configurarla como cuenta cerrada, lo que tiene por consecuencia que su información sea visible no solo a los usuarios de la plataforma social, sino a todo usuario con acceso a Internet; de igual forma, no existía justificación del bloqueo, ya que no se acreditó nunca por el Fiscal General, la existencia de un "comportamiento abusivo" por el quejoso.

De este asunto, la Segunda Sala emitió la siguiente Tesis Aislada de rubro **LIBERTAD DE EXPRESIÓN Y DERECHO DE ACCESO A LA INFORMACIÓN EN REDES SOCIALES. NO PROTEGEN EL COMPORTAMIENTO ABUSIVO DE LOS USUARIOS,** que señala:

> "La libertad de expresión y el derecho de acceso a la información, reconocidos por el artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, se han potencializado gracias a las oportunidades de fácil acceso, expansión e inmediatez que el internet y las redes sociales brindan. No obstante, debe reconocerse también la posible comisión de abusos dentro de esos medios virtuales que se ven agravados por las

---

Ley de Amparo: https://www.scjn.gob.mx/sites/default/files/listas/documento_dos/2019-03/AR%201005-2018%20..pdf

[28] *Ibidem*, p. 43-45.

mismas razones. Por tanto, **las interacciones dentro de la comunidad digital no pueden ser ajenas a los límites y estándares de protección de los derechos fundamentales.** En el caso de las redes sociales, existe la posibilidad de encontrar comportamientos abusivos derivados de su propia naturaleza, como son la comunicación bilateral y el intercambio de mensajes, opiniones y publicaciones entre los usuarios, razón por la cual el receptor de estos contenidos puede estar expuesto a amenazas, injurias, calumnias, coacciones o incitaciones a la violencia, que pueden ir dirigidas tanto al titular de la cuenta como a otros usuarios que interactúen en ella; en consecuencia, **es posible que los comportamientos abusivos puedan ocasionar una medida de restricción o bloqueo justificada, pero para que ésta sea válida será necesario que dichas expresiones o conductas se encuentren excluidas de protección constitucional en términos del artículo 6o. mencionado y de los criterios jurisprudenciales emitidos por la Suprema Corte de Justicia de la Nación** que rigen en la materia. Sin embargo, debe dejarse claro que las expresiones críticas, severas, provocativas, chocantes, que puedan llegar a ser indecentes, escandalosas, perturbadoras, inquietantes o causar algún tipo de molestia, disgusto u ofensa no deben ser consideradas un comportamiento abusivo por parte de los usuarios de la red." [29]

Con este criterio, podemos observar que es posible el bloqueo y restricción cibernético en caso de "comportamiento abusivo", siempre y cuando estén excluidas del derecho fundamental de "libertad de expresión" previsto por el artículo 6º constitucional. Si a simple vista no se define que debe considerarse por "comportamiento abusivo", hay que concluir que éste no incluye "las "expresiones críticas, severas, provocativas, chocantes, que puedan llegar a ser indecentes, escandalosas, perturbadoras, inquietantes o causar algún tipo de molestia, disgusto u ofensa".

Ante el pronunciamiento de la Segunda Sala, valdría recordar la jurisprudencia que la Primera Sala emitió en el 2013, bajo el rubro **LIBERTAD DE EXPRESIÓN. LA CONSTITUCIÓN NO RECONOCE EL DERECHO AL INSULTO** que establece que las ofensas o insultos no pueden faltar al respeto

[29] **LIBERTAD DE EXPRESIÓN Y DERECHO DE ACCESO A LA INFORMACIÓN EN REDES SOCIALES. NO PROTEGEN EL COMPORTAMIENTO ABUSIVO DE LOS USUARIOS.** 2ª.XXXVIII/2019 (10ª.), S.J.F., 7 de junio de 2019, Décima Época, Segunda Sala.

al honor y reputación**.** Es importante considerarla porque se aclara que la Constitución Política de los Estados Unidos Mexicanos no reconoce un derecho al insulto o injuria gratuita, lo que permite es el uso de la libertad de expresión cuando participe en un debate público, para criticar o atacar mediante el empleo de términos excesivamente fuertes, con cierta dosis de exageración e incluso de provocación**,** sin faltar al respeto a la reputación y derechos de terceros. Se destaca que dicha jurisprudencia derivó de cinco amparos directos que reclamaban daño moral en el uso de la libertad de expresión ejercido en medios impresos como periódicos, por lo que en el medio electrónico y del ciberespacio debería considerarse el mismo límite a la libertad de expresión, esto significa al honor y reputación de una persona, como refiere el criterio:

> "el derecho al honor prevalece cuando la libertad de expresión utiliza frases y expresiones que están excluidas de protección constitucional, es decir, cuando sean absolutamente vejatorias, extendiendo como tales las que sean: a) ofensivas u oprobiosas, según el contexto; y b) impertinentes para expresar opiniones o informaciones, según tengan o no relación con lo manifestado". [30]

V. Conclusiones

Como fue expuesto, el ciberderecho es una disciplina jurídica nueva que se encuentra mundialmente en desarrollo, algunos países con mayor exposición que otros, en virtud de su raíz cultural y social, pero que está perfilada a compartir principios y derechos comunes, por el uso universal con el que fue concebido su diseño.

México no puede quedarse atrás, debe alinearse a los pioneros y formar a todo el sector público y privado para que esté en posibilidad de competir,

[30] **LIBERTAD DE EXPRESIÓN. LA CONSTITUCIÓN NO RECONOCE EL DERECHO AL INSULTO** Jurisprudencia (constitucional) 1a/J.31/2013 (10a), S.J.F., Libro XIX, Abril de 2013, Tomo 1, Pag. 537, Décima Época, Primera Sala.

interactuar y defenderse en este nuevo terreno digital; en la medida que considere los modelos, principios, instituciones, sentencias y demás fuentes que el derecho comparado ha tenido bien compartir, estará en mejores posibilidades de formular un adecuado postulado jurídico que precise el catálogo de actuación al cual debe apegarse el cibernauta, de lo contrario, seguiremos enfrentando u observando importantes ataques en el ciberespacio que violenten derechos fundamentales.

El reto no está en prevenir ataques cibernéticos, sino en crear y fomentar una cultura ética del cibernauta que busque la sana convivencia en apego a un marco jurídico que procure el mejor desarrollo del hombre en el medio digital.