Tópicos de Política Criminal 2. Ciencia y Tecnología

Coordinador: José Antonio Álvarez León

UNAM POSGRADO
Derecho

TOPICOS DE POLÍTICA CRIMINAL 2.
CIENCIA Y TECNOLOGÍA

TOPICOS DE POLÍTICA CRIMINAL 2
CIENCIA Y TECNOLOGÍA

José Antonio Alvarez León
Coordinador

Universidad Nacional Autónoma de México
Programa de Posgrado en derecho
México, 2021

Primera edición, 2021

Topicos de Política Criminal 2. Ciencia y Tecnología

Coordinador:
José Antonio Alvarez León

Diseño de Portada:
Patricia Alajandra Ibáñez Alvarez

Maquetación:
José Manuel Guevara García

ISBN versión impresa: 978-607-30-4716-6
ISBN: versión digital: 978-607-30-4682-4

Derechos reservados 2021. Todos los derechos reservados conforme a la ley. Las características de esta edición, así como su contenido, no podrán ser reproducidas o transmitirse bajo ninguna forma o por ningún medio, electrónico, mecánico, incluyendo fotocopiado y grabación, ni por ningún sistema de almacenamiento y recuperación de información sin permiso por escrito del propietario del Derecho de Autor.

© Universidad Nacional Autónoma de México, Ciudad Universitaria, Delegación Coyoacán, C.P. 04510, Ciudad de México, a través de la Coordinación del Programa de Posgrado en Derecho de la UNAM, Unidad de Posgrado, Edificio "F", Circuito de Posgrado, Ciudad Universitaria, Delegación Coyoacán, C.P. 04510, Ciudad de México

© José Antonio Alvarez León

Hecho en México

Directorio

Enrique Graue Wiechers
Rector

Leonardo Lomelí Vanegas
Secretario General

Patricia Dolores Avila Aranda
Coordinadora General de Estudios de Posgrado

Fernando Guadalupe Flores Trejo
Coordinador del Programa de Posgrado en Derecho

Entidades

Raúl Contreras Bustamante
Facultad de Derecho

Manuel Martínez Justo
Facultad de Estudios Superiores Acatlán

Fernando Macedo Chagolla
Facultad de Estudios superiores Aragón

Pedro Salazar Ugarte
Instituto de Investigaciones Jurídicas

Hector Alejandro Ramírez Medina
Coordinador editorial

Índice

Prólogo 11
José Antonio Alvarez León

La política criminal en méxico para la prevención y combate del *phishing* cometido a través de *app´s* 15
Ana Beatriz Castrejón Díaz / David Chacón Martínez

Inteligencia geoespacial y política criminal en méxico 39
José Antonio Alvarez León / Karla Santamaría Roa

Sistema financiero mexicano. retos de seguridad hacía la transformación digital 71
José Alejandro González Reyna / Stephanie Cervantes Razo

Política criminal y violencia en el espacio virtual 101
Anahy Rodríguez González / Rodolfo Alexandro Buendía Castro

La identidad digital como garantía constitucional y un medio para la prevención del delito 125
David Alejandro Parada Sánchez / Ingrid Haide Díaz León

Reflexiones en torno a la prevención del delito de trata de niñas menores de edad a través de las redes sociales 149
José Antonio Alvarez León / Carla María Escoto

Cibercriminalidad financiera: el papel de las criptomonedas en el lavado de dinero 183
Silke Mora López / Héctor Alejandro Ramírez Medina

La fragmentación de la delincuencia organizada y su relación con la violencia en el contexto del covid-19 en méxico 207
Magdalena Alcocer Vega / Mariana Lucía Pérez Pérez

Los retos del derecho ante las nuevas tecnologías como generadoras de conductas delictivas 229
Luis Ángel Morales Cortez / Lidia Chávez Fonseca

Nada nuevo es que nos vigilen. el uso de drones y su regulación 255
José Antonio Alvarez León / Vianey Vega Maldonado

El uso de las tecnologías de la información y comunicación en la política criminal: control y vigilancia 277
Jorge Ignacio Jiménez Martínez / Roberto Álvarez Manzo

PRÓLOGO

Después de la guerra fría la globalización trajo consigo un impulso inédito para la humanidad. El desarrollo de los nuevos patrones de acumulación sólo fue posible con la ciencia y la tecnología en el campo militar, dejando el desarrollo comercial en manos de los civiles. La nueva era digital cambió la industrialización, sistematizó prácticamente todos los campos de ella e impulsó sin precedentes la era de las comunicaciones satelitales y electrónicas.

El mundo cambió. Las fronteras físicas dejaron de serlo y las relaciones personales cambiaron a nuevos caminos sin límites para encontrarse con sus semejantes en la inmediatez que permitió el internet. Los cambios impulsados con las nuevas tecnologías de la información y la comunicación no pudieron escapar a la condición humana donde se gesta la antítesis de las virtudes del hombre, al progreso, al bien, a la satisfacción, la ayuda, la honradez, etcétera. Así, el nuevo desarrollo de la humanidad trajo también en la nueva vida paralela a la realidad física, la deshumanización, la soledad, el desencuentro, las falsas realidades, pero aún peor, la vulneración de los nuevos bienes por tutelar, el ciberdelito, la estafa, la suplantación de identidad, el ataque a las instituciones, el mundo subterráneo (*Deep web*).

En el mundo virtual, la ciberdelincuencia, la estafa, la suplantación de personas, los ataques a las instituciones, los robos, los acosos virtuales y otra muchas conductas delictivas se desarrollaron a la par de las tecnologías , pero aún más se conectaron con el mundo físico (real) para ampliar sus modus operandi en conductas peligrosas y muy lesivas como la trata de personas, el tráfico de armas, la comercialización de drogas e incluso, se pone constantemente en riesgo a los estados nacionales.

El derecho penal por su propia naturaleza ha necesitado de la acreditación fáctica de las conductas delictivas, por tanto ha ido de la mano de los avances científicos y tecnológicos, haciéndolo un

derecho penal científico. Consecuentemente las prácticas policiacas y de reclusión carcelaria también se han ido adaptando a la ayuda que estos cambios proporcionan.

La política criminal contemporánea también se ha ajustado en sus procesos y definiciones para que la ciencia y la tecnología puedan ser de utilidad en las estrategias de prevención del delito ex ante y ex pos al derecho penal. En México algunas herramientas tecnológicas aún son vista con recelo a su implementación por parte del Estado que inscribe el debate en el contexto de la lesión de derechos humanos, control de la detención, uso desmedido de la violencia; discursos que evidencian la incapacidad del estado mexicano para enfrentar con velocidad los cambios, pues los delincuentes aceleran sus pasos respecto de la justicia. Pero también queda de manifiesto que la sociedad mexicana es contradictoria y acomodaticia cuando se clama justicia, usando las nuevas herramientas de control que deberían de ser aceptadas.

En este texto, la intención es poner en la reflexión que, en la definición abierta de la política criminal la prevención social de la violencia y el delito requieren encontrar tanto auxilio como eco con el uso de la tecnología. Es importante señalar que mucha de la tecnología que hoy está en manos militares o privadas puede y debe de ser parte de las estrategias públicas de control del delito. Se busca que el lector pueda pasar por algunos tópicos donde su vida pueda verse afectada o resuelta, impulsando el cambio que de igual forma es ya inminente.

La historia de nuestro país se ha escrito desde el poder público en un halo de corrupción e impunidad de forma atroz, lo que ha generado que el fenómeno del delito y la violencia se han vuelto casos endémicos. Hoy, además de la actitud de cambio y la renovación ética de valores para que funcione la participación ciudadana en las estrategias preventivas, se requieren resultados contundentes en el mundo físico y en la red; así como será necesario la tecnificación del poder penal formal del Estado en pro de sus postulados demo-

críticos de justicia que son las aspiraciones ciudadanas amen de un mínimo de certeza y seguridad.

Tópicos de Política Criminal 2, Ciencia y Tecnología, son un acercamiento desde la multidisciplina, lo que podrá enriquecer la forma de ver los problemas que desde esta disciplina requieren sin demora de la intervención de los nuevos saberes científicos, abriendo con ello espacios para la reflexión y la propuesta.

Es un texto compuesto de artículos donde se impulsa también el compromiso universitario de acompañar a jóvenes universitarios en la iniciación a la investigación, por tal motivo el presente libro es escrito en binomios profesor – alumno (de diferentes niveles licenciatura, especialidad, maestría y doctorado). Quienes aquí escriben son en su mayoría integrantes del sistema UNAM, pero también se ven enriquecidos con invitados de la Universidad Anáhuac y el talento de la Universidad Autónoma Metropolitana en su edición y diseño.

José Antonio Alvarez León

LA POLÍTICA CRIMINAL EN MÉXICO PARA LA PREVENCIÓN Y COMBATE DEL *PHISHING* COMETIDO A TRAVÉS DE *APP´S*

Ana Beatriz Castrejón Díaz*
David Chacón Martínez**

El hombre ha nacido libre, y sin embargo,
vive en todas partes entre cadenas.
Juan Jacobo Rousseau.

SUMARIO**:** I. Introducción. II. Historia y Evolución. III. ¿Cuál ha sido el tratamiento del "*PHISHING*" en la actualidad? IV. Phishing como delito en México. V. La política criminal implementada en México para el combate del robo de identidad a través del *PHISHING* en las nuevas tecnologías. VI. Regulación del Robo de Identidad a nivel Federal. VII. Regulación del Robo de Identidad a nivel Estatal. VIII. Protección de Datos Personales en México. IX. Política Criminal Internacional Sobre Delitos Electrónicos. X. Conclusiones. XI. Fuentes de Información.

I. INTRODUCCIÓN

A través de los años el mundo se ha transformado mediante la innovación en materia tecnológica, es así que la creación de nuevas herramientas y la utilización de la red ha permitido cada vez más que en distintas áreas se implementen aplicaciones para casi todo tipo de actividad, desde la financiera hasta aquellas con fines recreativos.

---

* Ana Beatriz Castrejón Díaz. Abogada Postulante. Profesora en la Licenciatura en Derecho. Fes Acatlán. UNAM.
** David Chacón Martínez. Estudiante de la Licenciatura en Derecho. Fes Acatlán. UNAM.

Éstas nuevas herramientas han favorecido la comunicación y la facilidad para que la sociedad pueda realizar diversas actividades a distancia, en menor tiempo y de forma amigable. En esta tesitura, y a pesar, que las nuevas aplicaciones (*APP´S*) han sido útiles, y tienen grandes ventajas, las conductas delictivas han afectado su uso, creando daños entre los usuarios.

Es así que uno de los principales problemas mundiales de la actualidad en el contexto de política criminal con enfoque tecnológico ha sido el *"PHISHING"* denominado como una conducta delictiva de la era digital, y con la que los países se han enfrentado, obligándoles a legislar con la finalidad de proteger a los usuarios en el uso de *APP´S*.

Por lo anterior, en este artículo nos enfocaremos en explicar y explorar este delito que ha ido evolucionando a través de internet durante varios años comenzando en la década de los noventas y afectando en la actualidad. En este contexto, es indispensable conocer los antecedentes históricos y el proceso evolutivo para entender en lo que se ha convertido hoy en día y cómo avanza, aunado a los adelantos tecnológicos que se vislumbran cotidianamente, agregando factores como la globalización de las redes informáticas y los cambios provocados por la digitalización y la falta de educación cibernética mundial.

Convencidos de la necesidad de aplicar, con carácter prioritario, una política criminal, con el objeto de proteger a la población mexicana frente a la ciberdelincuencia el análisis desde el punto de vista jurídico es indispensable para poder sopesar todas aquellas situaciones que se pueden presentar sobre esta práctica delincuencial, que se ha desarrollado vía electrónica como una nueva forma de vulneración a los bienes jurídicos tuteados que hoy conocemos.

II. HISTORIA Y EVOLUCIÓN

La primera referencia al término *"PHISHING"* se escuchó a mediados de la década de los noventa en un *blog* cibernético que frecuentaban agrupaciones de personas que se llamaban a sí mismas "crackers" (que según su adaptación del inglés al español son personas que rompen algún tipo de seguridad). Estos tenían la intención de intervenir las cuentas de correo electrónico de la empresa America Online (AOL) y robar la identidad de la cuenta a sus usuarios.

El *modus operandi* de los *"crackers"* consistía en ponerse en contacto con los usuarios vía correo electrónico, haciéndose pasar por un empleado de AOL y creando una cuenta de *e-mail* falsa con el nombre de la empresa, en estos correos electrónicos solicitaban información sobre las cuentas como nombres de usuarios y contraseñas; los mensajes emitidos contenían diferentes excusas como la verificación de la cuenta o corroborar la dirección de facturación.

Una vez que la víctima entregaba esta información confidencial, el *"PHISHER"* tenía acceso a su cuenta y a la información guardada en ella y así ser usada con cualquier otra finalidad.[1]

Esto fue posible debido a que los antiguos servidores de internet y empresas dedicadas a estos servicios, no contaban con medios de seguridad para identificar cuentas de correo apócrifas y los pocos usuarios de estos medios electrónicos eran muy vulnerables y propensos a ser víctimas de algún delito económico o de robo de identidad.

---

1 https://www.websecurity.digicert.com/es/mx/security-topics/brief-history-phishing-part-1. Consulta 11 de enero de 2021. 11: 58 hrs.

III. ¿CUÁL HA SIDO EL TRATAMIENTO DEL "*PHISHING*" EN LA ACTUALIDAD*?*

Se puede definir el *"PHISHING"* como el proceso mediante el cual una persona es contactada por vía electrónica por alguien pretendiendo ser una institución legítima con la finalidad de obtención de datos personales, como pueden ser cuentas bancarias, contraseñas, información de familiares y/o amigos, así como un sin fin de datos de índole privada. Esta información obtenida de manera fraudulenta es usada para acceder a las cuentas de la víctima y hacer mal uso de estas en cualquier sentido maligno.

El actual *"PHISHING"* se ha desarrollado de una manera mucho más profesional, tanto que se ha visto favorecido por el avance tecnológico y su globalización. Este fenómeno ha configurado nuevas formas y nuevas técnicas según el desarrollo tecnológico, esto significa que un ataque de *"PHISHING"* puede llegar a adquirir tintes de ingeniería informática y social, como podrían ser información a la que pueden tener fácil acceso a través de las redes sociales y mencionar cualquier tipo de información, como amigos en común o cuentas de correo para crear un vínculo y generar confianza con la víctima.

El *"PHISHING"* ataca a los principales usuarios de todo tipo de aplicaciones (*Apps*), cuyas afectaciones que a nivel internacional han ido en aumento creando perdidas económicas millonarias y gran impacto social a las compañías y a los usuarios. A la par de esto, la evolución de este delito cibernético, también han aumentado los métodos de prevención del mismo.

Esto se ha convertido en un problema global, de índole internacional y los países víctimas de estos ataques deben trabajar juntos y en conjunto con las empresas prestadoras de estos servicios, para obtener todo tipo de información sobre esta nueva forma de delito y así poder lograr una batalla exitosa contra éste.

IV. *PHISHING* COMO DELITO EN MÉXICO

La incorporación en México de las nuevas tecnologías a la vida moderna ha traído consigo una nueva problemática jurídica que merece la tipificación de un nuevo delito del género cibernético, surgiendo una serie de novedosos planteamientos jurídicos.

Hoy en día el *PHISHING* en nuestro país deber ser contemplado y adecuado a una serie de delitos de orden común como la usurpación de identidad o el fraude, entre otros, sin embargo, no se ha implementado una ley donde se contemple de manera estricta la conducta del *PHISHING*.

En palabras de Jorge Esteban Cassou Ruiz:

> Lo ideal no es contemplar una serie de figuras jurídicas diseminadas a lo largo de diversos ordenamientos que conformen el sistema jurídico mexicano, sino que deben incluirse en una ley especial en la que de modo sistematizado aglutinen las diferentes conductas lesivas, esa clasificación y distinción no deberá ser determinante y terminal, porque el desarrollo y la innovación tecnológica, de modo irremediable conduce a que día a día, surjan nuevas y variadas conductas que generen afectación a terceros, por lo que es mejor no establecer conductas casuísticas en dicha ley especial.[2]

Actualmente nos encontramos con la problemática para poder sancionar de manera adecuada todas las conductas delictivas que puedan cometerse a través de internet, plataformas digitales y aplicaciones (*apps*), por lo que es necesario que demos herramientas legislativas a los jueces para lograr una impartición eficaz de la justicia.

---

2 *(*Cassou Ruiz , J. E. (2009). Delitos Informáticos en México . *Revista del Instituto de la Judicatura Federal* , *28*, 207-236. https://doctrina.vlex.com.mx/vid/delitos-informaticos-mexico-75456707) Consulta 11 de enero de 2021. 12:02 hrs.

V. LA POLÍTICA CRIMINAL IMPLEMENTADA EN MÉXICO PARA EL COMBATE DEL ROBO DE IDENTIDAD A TRAVÉS DEL *PHISHING* EN LAS NUEVAS TECNOLOGÍAS.

De conformidad con el artículo 4º de la Constitución Política de los Estados Unidos Mexicanos que prevé *"Toda persona tiene derecho a la identidad…"* el Estado está obligado a implementar diversos mecanismos con el objeto de garantizar la efectividad del que hoy puede ser llamado *derecho humano a la identidad*.

En la actualidad, el uso de las nuevas tecnologías como las *APP* - aplicación de software diseñada para ejecutarse en los smartphones (teléfonos inteligentes), tabletas y otros dispositivos móviles[3]- en México, ha provocado el aumento del robo de identidad, que desde luego, atenta de forma directa al derecho humano a la identidad, al patrimonio y en algunos casos hasta la reputación.

En esta tesitura, el robo de identidad de conformidad con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales es "la apropiación de la identidad de una persona, para hacerse pasar por ella, asumir su identidad frente a terceros públicos o privados, a fin de obtener ciertos recursos o beneficios a su nombre. El robo de identidad implica la obtención y uso NO autorizado e ilegal de datos personales."[4]

VI. REGULACIÓN DEL ROBO DE IDENTIDAD A NIVEL FEDERAL.

A pesar que el robo de identidad mediante *"PHISHING"* es un problema que afecta a gran número de mexicanos y, vistas las circunstancias actuales en las que el uso de la tecnología se ha

3 http://www.lineaverdeceutatrace.com/lv/consejos-ambientales/apps-ambientales/que-es-una-app.asp. Consulta 21 de agosto de 2020. 13: 20 hrs.

4 http://inicio.ifai.org.mx/DocumentosdeInteres/Guía_Prevenir_RI.pdf. Consulta 21 de agosto de 2020. 10: 00 hrs.

vuelto indispensable, a la fecha no se ha tipificado como delito en el Código Penal Federal, toda vez que el proyecto que fue intentado hace algunos años, únicamente fue aprobado por la Cámara de Diputados, por lo que la iniciativa quedó trunca.

Es así que la falta de regulación a nivel penal federal causa una laguna jurídica que obliga a los afectados a identificar algún delito que pueda tener similitud con la afectación directa cometida por el *"PHISHING"* y su robo de identidad, como podría ser el delito de fraude.

En este sentido, entonces ¿qué ordenamientos jurídicos a nivel federal podemos encontrar para proteger a los usuarios de *APP´s* en el caso de ser víctimas de robo de identidad a través del *"PHISHING"*?.

La Ley de Instituciones de Crédito que en su artículo 112 *Séptimus* prevé la figura de *"identidad falsa o suplantada"*, como a continuación se puede apreciar:

> *Artículo 112 Séptimus.- Se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientas mil Unidades de Medida y Actualización, a quien utilice u obtenga, por sí o a través de interpósita persona, cualquier servicio o producto financiero proporcionado por alguno de los sujetos a que se refiere el artículo 3 de esta Ley o por una autoridad financiera o alguna de sus áreas, bajo una identidad falsa o suplantada.*[5]

Por su parte, el Código Fiscal de la Federación en el artículo 110 fracción VII prevé lo siguiente:

> Artículo 110.- Se impondrá sanción de tres meses a tres años de prisión, a quien:
>
> …
>
> VII. A quien otorgue su consentimiento para llevar a cabo la suplantación de su identidad.[6]

5 Ley de Instituciones de Crédito. Fuente electrónica: Consulta 21 de agosto de 2020. 10: 00 hrs.

6 Código Fiscal de la Federación. Consulta 21 de agosto de 2020. 12:15 00 hrs.

Por otro lado, es importante destacar que como política pública del Estado, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, como órgano constitucional autónomo, se encarga de orientar e implementar información para la prevención del robo de identidad, a través de todas las recomendaciones e inclusive guías que publica para prevenir a los usuarios sobre el robo de identidad e incentivar al cuidado de los datos personales, por ejemplo *La Guía para Prevenir el Robo de Identidad.*[7]

De lo anterior, es evidente que la regulación a nivel federal es insuficiente para considerar que el Estado Mexicano salvaguarda de forma óptima la identidad de las personas, ya que deja a un lado las conductas ilícitas cometidas con el *"PHISHING", por lo que* se considera que, aunque han existido buenos avances, es menester que el Estado refuerce la política pública y criminal contra esta conducta.

VII. REGULACIÓN DEL ROBO DE IDENTIDAD A NIVEL ESTATAL.

Ahora bien, por lo que hace a las entidades federativas, se puede encontrar regulado en sus Códigos Penales la protección de la identidad, por ejemplo, en el Código Penal para el Distrito Federal (Ciudad de México) se prevé en el Capítulo III el delito de USURPACIÓN DE IDENTIDAD que a la letra dice:

> ARTÍCULO 211 BIS. Al que por cualquier medio usurpe, con fines ilícitos, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación en su identidad, se le impondrá una pena de uno a cinco años de prisión y de cuatrocientos a seiscientos días multa.
> Se aumentarán en una mitad las penas previstas en el párrafo

7 http://inicio.ifai.org.mx/DocumentosdeInteres/Guía_Prevenir_RI.pdf. Consulta 11 de enero de 2021. 12: 17 hrs.

> anterior, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito establecido en el presente artículo.[8]

Otro ejemplo, lo podemos encontrar en el Código Penal del Estado de México, que al igual que la Ciudad de México se tipifica como "usurpación de identidad", y que se transcribe a continuación:

> Artículo 264.- Se le impondrán de uno a cuatro años de prisión y de cien a quinientos días multa, a quien ejerza con fines ilícitos un derecho o use cualquier tipo de datos, informaciones o documentos que legítimamente pertenezcan a otro, que lo individualiza ante la sociedad y que le permite a una persona física o jurídica colectiva ser identificada o identificable, para hacerse pasar por él.
> Se equiparan a la usurpación de identidad y se impondrán las mismas penas previstas en el párrafo que precede prevista en el presente artículo a quienes:
> I. Cometan un hecho ilícito previsto en las disposiciones legales con motivo de la usurpación de la identidad;
> II. Utilicen datos personales, sin consentimiento de quien deba otorgarlo;
> III. Otorguen el consentimiento para llevar a cabo la usurpación de su identidad; y
> IV. Se valgan de la homonimia para cometer algún ilícito.
> Las sanciones previstas en este artículo se impondrán con independencia de las que correspondan por la comisión de otro u otros delitos.[9]

De las transcripciones efectuadas, se aprecia que el delito no está tipificado como un "robo de identidad" si no como una "usurpación de identidad". Esta diferencia ha sido criticada en algunos ámbitos, toda vez que se discute que el término adecuado es el robo y no la usurpación, sin embargo, se considera que es un gran avance para la protección de los usuarios de nuevas tecnologías.

---

8 Código Penal para el Distrito Federal. Consulta 21 de agosto de 2020. 11: 18 hrs.

9 Código Penal del Estado de México. Consulta 21 de agosto de 2020. 11: 18 hrs.

A comparación con el nivel federal, se considera que las entidades federativas han tenido un avance importante para el combate del *"PHISHING"* y la protección de la identidad de los ciudadanos, a pesar de las críticas que se han efectuado a sus legislaciones.

Cronológicamente el Código Penal del Estado de Sinaloa fue el primero en tipificar el Delito Informático y es el único que lo denomina en su artículo 217, el cual dice:

> ARTÍCULO 217.- Comete delito informático, la persona que dolosamente y sin derecho:
>
> I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o
>
> II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red. Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa[10]

VIII. PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

El "*PHISHING*" es una conducta directamente ligada a la vulneración jurídica del derecho a la protección de la información de datos personales consagrado en el artículo 6, fracción II de la Constitución Política de los Estados Unidos Mexicanos, que nos permitimos transcribir:

> Artículo 6º: "II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes."[11]

10 Código Penal para el Estado de Sinaloa. Consulta 21 de agosto de 2020. 11: 25 hrs.

11 Constitución Política de los Estados Unidos Mexicanos. Consulta 21 de agosto de 2020. 11: 30 hrs.

A nivel federal, de esta fracción se deriva en el 2017 la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que en su segundo artículo establece los objetos de dicha ley:

> Artículo 2º**:** Son objetivos de la presente Ley:
> **I.** Distribuir competencias entre los Organismos garantes de la Federación y las Entidades Federativas, en materia de protección de datos personales en posesión de sujetos obligados;
> **II.** Establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos;
> **III.** Regular la organización y operación del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a que se refieren esta Ley y la Ley General de Transparencia y Acceso a la Información Pública, en lo relativo a sus funciones para la protección de datos personales en posesión de sujetos obligados;
> **IV.** Garantizar la observancia de los principios de protección de datos personales previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia;
> **V.** Proteger los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de la Federación, las Entidades Federativas y los municipios, con la finalidad de regular su debido tratamiento;
> **VI.** Garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales;
> **VII.** Promover, fomentar y difundir una cultura de protección de datos personales;
> **VIII.** Establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio que correspondan para aquellas conductas que contravengan las disposiciones previstas en esta Ley, y

> **IX.** Regular los medios de impugnación y procedimientos para la interposición de acciones de inconstitucionalidad y controversias constitucionales por parte de los Organismos garantes locales y de la Federación; de conformidad con sus facultades respectivas.[12]

Es de vital importancia tomar en cuenta que las personas que llevan esta conducta irrumpen de manera ilegal a los servidores de particulares que contienen esta información para hacerse de información que pueda ayudar a conseguir la confianza de sus víctimas. A esto nos referimos con lo ya antes mencionado como "Ingeniería Social".

Dos de los artículos más destacables de la Ley hablan sobre las Sanciones por el uso inadecuado de los datos personales, en los artículos 163 y 165 encontramos lo que podrían ser los dispositivos legales que más se acerquen a la sanción penal sobre esta conducta actualmente en México.

> **Artículo 163**.- Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:
>
> I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;
>
> II. Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;
>
> III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

12 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Consulta 21 de agosto de 2020. 11: 30 hrs.

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;

VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la presente Ley;

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la presente Ley;

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la presente Ley;

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley;

XI. Obstruir los actos de verificación de la autoridad;

XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la presente Ley;

XIII. No acatar las resoluciones emitidas por el Instituto y los Organismos garantes, y

XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Ac-ceso a la Información Pública, o bien, entregar el mismo de manera ex-temporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las

> conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.
>
> En caso de que la presunta infracción hubiere sido cometida por algún integrante de un partido político, la investigación y, en su caso, sanción, corresponderán a la autoridad electoral competente.
>
> Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.
>
> **Artículo 165.** Las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a lo dispuesto por el artículo 163 de esta Ley, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.
>
> Dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.
>
> Para tales efectos, el Instituto o los organismos garantes podrán denunciar ante las autoridades competentes cualquier acto u omisión violatoria de esta Ley y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables.[13]

Debemos tomar en cuenta que la finalidad de esta ley no es atacar o prevenir los delitos cibernéticos, pero podría marcar la pauta para la creación de una ley de carácter federal que lo haga.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y los Organismos garantes que en conjunto forman el sistema nacional de transparencia están facultados para imponer medidas de apremio y sanciones

---

13 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Consulta 21 de agosto de 2020. 11: 30 hrs.

administrativas correspondientes para asegurar el cumplimiento de sus determinaciones.

Es así que se puede observar que el *"PHISHING"* es el resultado de una aplicación de distintas prácticas delictivas ya existentes pero englobada en una y con la característica especial de ser cibernética. Es aquí donde comienza el vacío legal por la falta de tipificación de esta conducta y muchas otras en materia de seguridad cibernética.

Es de vital importancia que México concentre un esfuerzo legislativo en estas conductas para evitar el acrecentamiento de estas prácticas en el futuro, la era digital está en auge y tenemos que dar una respuesta eficaz. Esto solo se logrará con la creación de una ley que tipifique las diferentes conductas y situaciones que se suscitan día con día en Aplicaciones (*APP´S*) y plataformas digitales.

Es indispensable ser enfáticos en el punto de convergencia entre estas dos situaciones dada la estrecha relación que la manipulación de datos personales y el *"PHISHING" comparten.* Los *crackers* han logrado una impresionante forma de estructura digital que avanza tan rápido como llegan los avances tecnológicos modernos. Su forma de ingeniería social desarrollada, junto con la falta de información sobre el uso de internet y sus avisos de privacidad han coadyuvado la extensión del "phishing" más rápido que la expansión de la cultura informática en el país, el mundo y la sociedad.

IX. POLÍTICA CRIMINAL INTERNACIONAL SOBRE DELITOS ELECTRÓNICOS

Si bien ya se ha dejado en evidencia el rezago legislativo de México en la materia. No podemos ignorar la política criminal implementada en otros países que están a la vanguardia.

Ahora bien, la Organización de las Naciones Unidas reconoce como delitos informáticos las siguientes conductas o acciones:

I) Los Fraudes cometidos mediante manipulación de computadoras: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común.

II) La manipulación de programas; este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas que tienen conocimiento especializados en programación informática.

III) La Manipulación de datos de salida; se efectúa fijando un objetivo al funcionamiento del sistema informático, el ejemplo más común es el fraude que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

IV) Fraude efectuado por manipulación informáticas de los procesos de cómputo.

V) Falsificaciones informáticas; cuando se alteran datos de los documentos almacenados en forma computarizada.

VI) Como instrumentos; las computadoras pueden utilizarse también para efectuar falsificación de documentos de uso comercial

VII) Sabotaje Informático; es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

VIII) Los Virus; Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos.

IX) Los Gusanos; los cuales son análogos al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

X) La Bomba lógica o cronológica; la cual exige conocimientos especializados ya que requiere la programación de la

> destrucción o modificación de datos en un momento dado del futuro.
>
> XI) Acceso no autorizado a servicios u sistemas informáticos; esto es por motivos diversos desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.
>
> XII) Piratas Informáticos o Hackers; este acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones. XIII) Reproducción no autorizada de programas informáticos de protección legal; la cual trae una pérdida económica sustancial para los propietarios legítimos.[14]

Por ejemplo, la Unión Europea, y de manera más específica España cuya inclusión en el Tratado de Conformación de la Unión Europea dio pauta para que existiera presión internacional europea para la homologación de leyes en conjunto, debido a la cercanía geográfica y la apertura comercial.

Es así que la Unión Europea a través de la Comisión Europea, planteó la aplicación de mejores medidas para reforzar la ciberseguridad (Comisión Europea, 2017c: 14-23).

> Tomando como base la labor de los Estados miembros y de la asociación público-privada, la capacidad de ciberseguridad de la UE se seguirá reforzando a través de una red de centros de competencia en ciberseguridad, cuyo eje será un Centro Europeo de Competencia e Investigación en Ciberseguridad. Esta red y su centro estimularían el desarrollo y el despliegue de tecnología de la ciberseguridad y complementarían los esfuerzos de capacitación en este ámbito a nivel nacional y de la UE[15]

---

14 https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap4.htm#4_1 . Consulta 21 de agosto de 2020. 11: 30 hrs.

15 Comunicación conjunta al Parlamento Europeo y al Consejo. Resiliencia, disuasión y defensa: fortale-cer la Ciberseguridad de la UE, Bruselas, 13.9.2017, *op. cit.*, pp. 11-23. Consulta 21 de agosto de 2020. 11: 30 hrs.

Dentro de esta recomendación se exhortaba a los Estados miembros al trabajo conjunto y a la homologación de procesos y leyes penales para volver más eficaz la lucha contra la ciberdelincuencia.

El trabajo de los Estados miembros y la Unión Europea en la lucha contra la delincuencia informática ha sido muy positivo durante los últimos años, mediante la aplicación de instrumentos normativos, iniciativas, políticas y proyectos para mejorar la calidad de vida de los ciudadanos europeos, haciéndola más segura ante la proliferación de las actividades delictivas informáticas. A pesar de los grandes logros conseguidos en los últimos años en la lucha contra la ciberdelincuencia, todavía queda mucho trabajo por realizar, y por ello debemos de hacer frente a una serie de retos en el futuro más cercano.

Uno de los puntos principales del trabajo que está realizado el Parlamento Europeo, se centra en la dificultad de Persecución de los delitos informáticos, pues ha ido más allá de la jurisdicción de un solo país, tomemos en cuenta que el acercamiento del mundo gracias a los medios digitales, también ha permitido la comisión de las conductas, por obvias razones han traspasado fronteras.

1. Política criminal contra el *PHISHING* en España.

El combate que España ha planteado contra el *phishing* tiene como fundamento toral dos instrumentos jurídicos:

- La Decisión Marco del Consejo de la Unión Europea sobre "la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo", de fecha 28 de mayo de 2001; y
- El Código Penal.

En esta tesitura, el artículo 3º de la Decisión Marco del Consejo de la Unión Europea, prevé lo siguiente:

> Artículo 3. Delitos relacionados con equipos informáticos
> *Cada Estado miembro adoptará las medidas necesarias para garantizar que las siguientes conductas sean delitos penales cuando se produzcan de forma deliberada:*

> realización o provocación de una transferencia de dinero o de valor monetario que cause una pérdida no autorizada de propiedad a otra persona, con el ánimo de procurar un beneficio económico no autorizado a la persona que comete el delito o a terceros, mediante:
> - la introducción, alteración, borrado o supresión indebidos de datos informáticos, especialmente datos de identidad, o - la interferencia indebida en el funcionamiento de un programa o sistema informáticos.[16] [Énfasis añadido].

De la transcripción elaborada con anterioridad, es importante destacar que la Unión Europea remarca que los Estados deben regular y castigar cualquier tipo de alteración, inducción o suplantación de identidad que se dé a través de equipos informáticos, lo anterior, desde luego fue una implementación jurídica loable, y adecuada con la transformación y evolución tecnológica por la que transitaba y sigue haciéndole no solamente la Unión Europea, también el mundo entero. Es menester observar que la Decisión Marco del Consejo de la Unión Europea es claro al señalar las conductas y los medios de los que se pueden hacer valer los *phishers* con la intención de crear conductas fraudulentas afectando el patrimonio de los diferentes usuarios de sistemas electrónicos, y a la fecha es tan amplia que sin duda regula también el uso de las *APP* (aplicaciones).

Ahora bien, el sistema jurídico de España, persigue y castiga las conductas del *phishing* a través del artículo 248 del Código Penal, que prevé lo siguiente:

1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en per-juicio propio o ajeno.

2. También se consideran reos de estafa:

> • Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una

16 https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32001F0413. Consulta 12 de enero de 2021. 13: 04 hrs.

transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

• Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

• Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

De conformidad con la Licenciada en Derecho y en Criminología María Victoria Rodríguez Caro "El ámbito de aplicación del tipo es tan amplio como para englobar los desplazamientos patrimoniales inconsentidos que se producen por medios informáticos. En palabras del Tribunal Supremo: "Cuando la conducta que desapodera a otro de forma no consentida de su patrimonio se realiza mediante manipulaciones del sistema informático, bien del equipo, bien del programa, se incurre en la tipicidad del art. 248.2. También cuando se emplea un artificio semejante. Una de las acepciones del término artificio hace que este signifique artimaña, doblez, enredo o truco. El artificio es equivalente, a los efectos del contenido de la ilicitud, cuando el autor modifique materialmente el programa informático indebidamente o cuando lo utilice sin la debida autorización o en forma contraria al deber." (STS 860/08, 17-12).

Las diferencias entre el tipo de la estafa informática y la clásica que recoge el art. 248.1 CP son evidentes, pues afectan a elementos tan característicos de este delito como son el engaño y el error que generan el acto de disposición en perjuicio de la propia víctima o de un tercero, en cambio subsisten los elementos subjetivos del dolo y el ánimo de lucro. – En cuanto al engaño, es de destacar que la nueva figura pretende proteger el patrimonio de los ataques que propician las nuevas tecnologías, que se describen por el legislador como "manipulación informática o artificio semejante", incluyendo todos aquellos mecanismos que sean idóneos para conseguir esa

transferencia inconsentida de un activo patrimonial, que integra el acto de disposición y que provoca el enriquecimiento que el autor persigue"[17]

Si comparamos la legislación aplicable en España para combatir el *phishing* con la de México, podemos percatarnos que en México la regulación jurídica -que en su mayoría es de carácter penal-, no señala de manera específica las conductas ilegales identificadas con el *phishing*, tan es así que observamos que los afectados deben de llegar al extremo de intentar identificar la conducta que más se asimile con las reguladas en los Códigos Penales con la intención que pueda perseguirse e identificarse el delito.

El problema con la política criminal en México, es que se ha quedado relegada en relación con los avances tecnológicos que ha sufrido el mundo. Un claro ejemplo, lo podemos observar con el uso de *APP´s* para actividades diversas, desde transferencias bancarias hasta la propia implementación de los Estados en actividades administrativas o de impartición de justicia, ¿es suficiente la regulación jurídica con la que cuenta México para combatir el *phishing*? ¿Son claros los tipos penales y las medidas de protección para los usuarios de tecnologías de la información?

X. CONCLUSIONES

El *"PHISHING"* es una conducta delictiva que se lleva a cabo mediante el uso de internet afectando en sus bienes y derechos a los usuarios de distintas aplicaciones (*APP´S*). Actualmente en México no existe de manera precisa un ordenamiento jurídico que señale la conducta y las consecuencias jurídicas del *"PHISHING"* como delito, lo que implica que las personas que han sido afectadas por ésta conducta se encuentren obligadas a denunciar un delito que en

17 http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10617-estafa-informatica-el-denominado-phishing-y-la-conducta-del-ldquo%3Bmulero/. Consulta 12 de enero de 2021. 13: 04 hrs.

medida de lo posible se asemeje a los daños que han sufrido como consecuencia del *"PHISHING"*.

Es cierto que México cuenta con el organismo Constitucional Autónomo denominado INAI cuya función es la protección de datos personales –entre otras-, y que día con día realiza un esfuerzo para prevenir a los usuarios en el uso de las aplicaciones –*APP´S*- y la protección de su datos personales para evitar caer en las trampas de los *"PHISHERS"*, sin embargo, las acciones del INAI y la legislación que actualmente es aplicable para castigar al *"PHISHING"* no es suficiente para poder considerarse como una política criminal adecuada que combata de raíz al *"PHISHING"* y que salvaguarde los bienes y derechos de los usuarios de *APP´S*.

En efecto, a nivel internacional el castigo del *"PHISHING"* ha tenido un gran avance, como es el caso de España, regulación que se podría tomar como referencia para la implementación de política criminal adecuada contra el *"PHISHING"* en México.

Desde nuestro punto de vista, es indispensable ejercer presión en el sistema legislativo y judicial mexicano con la finalidad que el *"PHISHING"* sea prevenido y castigado, lo que desde luego conlleva la seguridad y certeza jurídica de los usuarios de las *APP´S*, e inclusive la confianza para aquellos emprendedores que estén considerando crear una.

Queda un largo camino por recorrer, sin embargo, con el adelanto en el uso de nuevas tecnologías se espera que la legislación responda con las necesidades de la sociedad mexicana en la actualidad.

XI. FUENTES DE INFORMACIÓN

(Cassou Ruiz ,J. E. (2009). Delitos Informáticos en México. *Revista del Instituto de la Judicatura Federal* , *28*, 207-236. https://doctrina.vlex.com.mx/vid/delitos-informaticos-mexico-75456707)

http://www.lineaverdeceutatrace.com/lv/consejos-ambientales/apps-ambientales/que-es-una-app.asp.

http://inicio.ifai.org.mx/DocumentosdeInteres/Guía_Prevenir_RI.pdf

http://inicio.ifai.org.mx/DocumentosdeInteres/Guía_Prevenir_RI.pdf

https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap4.htm#4_1

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32001F0413

http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10617-estafa-informatica-el-denominado-phishing-y-la-conducta-del-ldquo%3Bmulero/

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017JC0450

https://www.websecurity.digicert.com/es/mx/security-topics/brief-history-phishing-part-1

Ley de Instituciones de Crédito

Código Fiscal de la Federación

Código Penal para el Distrito Federal.

Código Penal del Estado de México

Código Penal para el Estado de Sinaloa prueba

Constitución Política de los Estados Unidos Mexicanos

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

INTELIGENCIA GEOESPACIAL Y POLÍTICA CRIMINAL EN MÉXICO

José Antonio Alvarez León*
Karla Santamaría Roa**

SUMARIO: I. Introducción. Crisis de sentido y de seguridad. II. Fragmentación del delito. III. Inteligencia geoespacial y su vínculo con política criminal. IV. Aplicaciones adicionales: inteligencia-política criminal. V. Referencias Internacionales e instituciones mexicanas, uso masivos. VI. Conclusiones. VII. Fuentes consultadas.

I. INTRODUCCIÓN. CRISIS DE SENTIDO Y DE SEGURIDAD

Durante la crisis de sentido de los estados latinoamericanos a finales de los años cincuenta y principios de los setentas, quedó en claro que el poder penal fue usado para reprimir y controlar los movimientos asistémicos que buscaban y reclamaban justicia social y reivindicaciones colectivas; para los años ochenta la fuerza punitiva de los estados fue más selecta y dirigida a la reivindicación de la democracia occidental particularmente la norteamericana en un afán hegemónico universal; rápidamente en los años noventa y producto de los cambios en los patrones de acumulación del capital y el posicionamiento de la ciencia y la tecnología (globalización)[1] como medios de producción en manos de los grandes capitalistas, el mundo experimentó un redimensionamiento del control en función del surgimiento de nuevas formas del actuar criminal trasnacional

---

*José Antonio Alvarez León. Profesor investigador en el departamento de Posgrado en Derecho y Política Criminal. Fes Acatlán UNAM.
**Karla Santamaría Roa. Egresada de la licenciatura en Inteligencia para la Seguridad por la Universidad Anáhuac Norte.

Cfr. Hinostroza, Fernando. "TLC en contexto de la globalización". *Revista "A"*, México UAM-AZC, 1992.

Al inicio del siglo XXI, el surgimiento del terrorismo como justificación de todas las amenazas se multiplicó en todo el mundo estrategias globales, regionales de seguridad que cambiarían la historia del poder penal mundial y local de forma inédita.

Bajo este contexto, los países en vías de desarrollo como México, sufrieron transformaciones político estructurales tan extremas e incompletas (sin alcanzar el desarrollo esperado) que dieron como resultado estados debilitados donde la inseguridad, la corrupción, la antidemocracia y la acumulación de reclamos sociales se volvieron una constate ascendente en la vida individuos y descendiente en el nivel de vida y de respuesta de los estados.

México, por sus propias condiciones históricas (por el surgimiento, evolución y declive de sus sistema presidencial)[2], incubó consigo flagelos peligrosos como la antidemocracia, la corrupción, los pactos y la impunidad desde las estructuras del gobierno con la delincuencia; las persecuciones políticas, las venganzas de Estado, la no renovación de las clases gobernantes, la desaparición de personas, la simulación del progreso, el genocidio (se exterminaron poblaciones de indígenas originarios), de grupos rebeldes al sistema y por supuesto de civiles inocentes.

Aunque en mucho parece increíble, el país creció en el siglo XX como nunca había hecho, sin embargo, el proyecto de país posrevolucionario nació enfermo, alcanzó su punto de mayor descomposición en los años setenta (crisis de sentido) y después en el periodo neoliberal de donde ha sido imposible ya dar vuelta atrás (la globalización y el terrorismo).

México en los 70s y 80s el uso del aparato penal y militar mexicano fue para perseguir, enjuiciar y eliminar opositores, en este

---

2 "…no es coherente mi justificable la complicidad del gobierno con las transnacionales y su medio privilegiado y su medio de difusión para atentar contra el Estado, negar su Revolución y liquidar la nacionalidad, la identidad cultural del pueblo proyecto que debiendo ser protegido por el poder que de él mismo emana, es convertido en materia de negocio o dejado a su suerte" (sic). *Apud* Del Palacio Díaz, Alejandro. *Agonía y muerte de la Revolución Mexicana*, México, UAM-AZC Esquemas.1991, p 98.

sentido se habla de un uso faccioso y autoritario de los aparatos represores del Estado. Sin embargo, desde el salinato y de forma muy puntual con el ascenso al poder de la derecha conservadora[3], el poder penal del estado mexicano, se fragmentó[4] de tal forma que el uso recurrente de la fuerza se dio de manera formal e informal de forma selectiva y en algunos casos discrecionales.

Estas crisis encontraron sustento en un régimen presidencial de poder omnipotente, donde el sistema penal se caracterizó por concentración de toda la fuerza material del Estado en manos de un solo hombre (presidente de la república) capaz de doblegar incluso a cualquier poder fáctico. En México el presidente de la república generó una existencia falaz de la división de poderes, pues fue capaz de imponer y controlar al poder judicial federal y de influir de forma directa en la designación de candidaturas a puestos de elección popular como senadores, diputados e incluso, en las mismas entidades federadas.

Con el cambio democrático en el año 2000[5] (como consecuencia del surgimiento de *gobiernos tecnocrático) se acelera la reforma del Estado en la estructura política y* se continuó el desmantelamiento de las estructuras económicas del Estado Social Mexicano[6]. Como ya se

3 Triunfo del partido Acción Nacional en el año 2000 y su continuidad en el período 2008-2012.

4 *Vid Infra* Punto II.

5 "El retorno del PRI fue, en sí mismo, un mensaje reprobatorio para la administración de Fox y Calderón. Con el primero llegaron la chabacanería, la improvisación ruinosa y los abusos de poder; la pareja presidencial, el *toallagate,* la ineptitud de los "súper gerentes"; el enriquecimiento claramente *explicable* de Manuel Bribiesca Sahagún y un largo etcétera que incluye la *inexplicable* bonanza de cuadros medios y altos…Con el segundo….el gabinete lleno de "leales" … que entregaron al final del sexenio un país más vulnerable en términos de seguridad y justicia ….muchos de esta segunda camada de panistas *empoderados* tampoco resistieron la tentación del dinero fácil con cargo al erario" (sic). *Apud,* Zárate, Alfonso. *Un gobierno fallido*. Peña Nieto y la sucesión presidencial de 2018, México, Temas de hoy. 2018, Pp 39-40.

6 " La irrupción de la tecnocracia en el régimen, acompañada de la pretensión ideológica de contraponer la administración a la política, como si la administración pública no fuera ya en sí misma una función política y expresión del ser del Estado y como si la política no fuera ya, de principio, una técnica, trae por consecuencia

dijo líneas arriba, la derecha siguió de forma ortodoxa la transformación del Estado revolucionario al Liberal, pero junto con ese cambio se recrudeció la impunidad y el saqueo en los niveles más altos del gobierno. La crisis de adaptación a la globalización, la impunidad rapaz con la miseria económica de escenario generalizado permitió que los poderes fácticos mafiosos se apoderaran de algunas zonas del territorio nacional y absorbieran los espacios de control de la delincuencia convencional generando que el delito se volviese un elemento cotidiano en la vida de los mexicanos.

La derecha radical en el poder enarboló como bandera de gobierno la lucha a la delincuencia trasnacional y local, usando las fuerzas armadas ante el debilitamiento de las estructuras policiales y el Ministerio Público, hechos que también fueron el discurso para realizar los cambios en el estado mexicano en los temas de justicia iniciados en 1994 con Ernesto Zedillo y que culminarían con los gobiernos de Felipe del Sagrado Corazón de Jesús, cumpliendo la reforma judicial del 2008, la implementación del modelo de seguridad basado en el Plan Mérida[7] y con la reforma a los derechos humanos del 2011; después, Peña Nieto mantendría el estado de cosas agudizando la conformación del estado mafioso.

Sin entrar en detalle diremos que México ha vivido la peor etapa de su historia en temas de seguridad después de la cruenta revolución mexicana (que fue una guerra civil). El mexicano ha tenido que aprender a vivir con el delito, la violencia y la inseguridad las cifras en uno delito u otro cambian, pero la constante general es que los delitos de impacto se volvieron progresivos alternando los sitios estadísticos entre uno y otro, de una región a otra del país.

---

la paulatina pero segura y acrecentada independencia de la administración del ejecutivo; pero lejos de significar su puesta a salvo de la política ha significado la ruptura de la unidad del poder del Estado …" *Apud* Del Palacio Díaz, Alejandro. *Del Estado de Derecho al Derecho del Estado*, México, Leega Omnibus, 1988. P 88.

7 "… lo ocurrido en el sexenio de Calderón: que en muy buena medida, "la guerra contra las drogas" nos fue impuesta desde Washington y sus agencias antinarcóticos"(sic),*Apud,* Zarate, Alfonso. *Op.Cit.* p 63.

La mafia operó desde la presidencia de la república recordando los viejos tiempos del Priismo donde un jefe policiaco encabezó el aparato policial en la ciudad (Durazo Moreno); siguiendo la misma tónica priista, Calderón[8], colocó como jefe de la policía federal a un mafioso que se encargaba paradójicamente de encabezar bandas de secuestradores y traficantes de drogas a la par de cuidar a la ciudadanía.

Como resultado de las política de guerra al crimen organizado 2006-12, México fue calificado en algunas regiones como Estado en descomposición y en general como el Estado que sin estar en conflicto bélico se volvió de los países más peligrosos del mundo (lo que ubico el inicio del sexenio de Peña Nieto en un proceso decadente)[9]. Se calcula que sólo en ese sexenio desaparecieron, murieron y fueron desplazados más de 75,000 personas con lo que se reabrió la penosa historia de los crímenes de estado "desaparición forzosa".

Bajo este panorama histórico pasado-presente, la incidencia delictiva mostraba y muestra tendencias progresivas de aumento. La inseguridad se convirtió un tema recurrente en los medios de comunicación al grado que el gobierno de Peña Nieto, impusiera la censura en las notas sobre delitos y violencia[10]; consecuentemente la inseguridad se volvió forma de calificación a los gobiernos en turno. La violencia local (municipios y estados) se volvió tan focalizada cómo dispersa. Las zonas urbanas y rurales fueron escenarios de la debacle del Estado ante el crimen.

---

8 "Calderón convirtió la seguridad pública en su obsesión. La dimensión del fracaso se apreciaba con el recuento de ejecuciones, secuestros y extorsiones, así como la "expropiación" de extensos territorios en los que, aún hoy, las bandas criminales imponen su ley." (sic). *Apud* Zárate, Alfonso. *Op. Cit,* p 40.

9 Estudio: México el segundo país más violento del mundo. *Cfr.*https://www.dw.com/es/estudio-m%C3%A9xico-es-el-segundo-pa%C3%ADs-m%C3%A1s-violento-del-mundo/a-38770281. Consultado: enero 5, 2021.

10 "El cambio de "tono" consistió en bajarle el volumen a la difusión de hechos delictivos. Los estrategas oficiales pensaban que el miedo de la sociedad era, principalmente, un problema de percepción alimentado por los medios". *Apud,* Zarate, Alfonso, *Op. Cit*, p 64.

El crimen convencional se fundió de lleno en con el crimen trasnacional ampliando los espectros de la delincuencia organizada, el poder delictivo se elevó exponencialmente, que ahora controla con igual violencia y terror en zonas urbanas, rurales, nichos de producción e incluso espacios públicos, se penetran todas las estructuras institucionales municipales, estatales y federales e incluso las organizaciones civiles de convivencia; los tentáculos del poder criminal vuelve una dicotomía de presencia y acción en la vida cotidiana, haciendo del *modus operandi*, un estilo de vida y una imposición de las formas cotidianas de vida.

Con una conducta delictiva se producen varios delitos como lo marca la ley (previsto en el concurso real e ideal de delitos), sin embargo, con esa conducta base, se genera un cadena de vida criminal que es capaz de tener no sólo ganancia exorbitantes, sino que permea las bases de vida más sencillas en una colonia, fraccionamiento, alcaldía o pueblo; en ella participan desde un niño que juega al balón (cómo halcón) en las calles hasta el jefe de plaza; con esto el concurso de delitos queda simplemente superado pues sus fines de identificación y de control de quienes cometen delitos a nivel procedimental no al ámbito criminal, hecho que deja fuera de poder penal las estructuras cambiando o entregando sólo a peones en la comisión de los delitos.

La vida mafiosa se mezcla con la vida común y corriente, generando poder fragmentado desde lo más pequeño a lo más poderoso. La agente común, tiene que aprender a distinguir dentro de su barrio o colonia a los mafiosos, a tolerarlos, a callar los comentarios que puedan correr a ellos y ponerlos en peligros (se controla la protesta de los colonos), se violan las leyes de la convivencia escrita y no escrita, la mafia está en las colonias pudientes y en los barrios más bajos. Como consecuencias tener control preventivo (al menos) es prácticamente imposible.

Las autoridades de seguridad pública también permeadas desde dentro de sus instituciones deberán enfrentan tres dificultades bá-

sicas: 1. La filtración de la información, 2. Los procedimientos de actuación con base en los derechos humanos y las exigencias del nuevo sistema de justicia penal, 3. Operar en reacción y disuasión de forma rápida en virtud de la taza porcentual de presencia de una un oficial por cierto número de habitantes, en un ciertas dimensiones territoriales (problema particularmente complejo en zonas densamente pobladas o muy abiertas).

II. FRAGMENTACIÓN DEL DELITO

La crisis de seguridad pública en nuestro país ha conducido a que el nuevo gobierno federal (2018-2020) haya calificado a los gobiernos estatales y a las administraciones federales que le precedieron cómo instituciones que volvieron al Estado Mexicano en una entidad mafiosa[11]. Lo real, es que se pasó de una forma única de identificación y concepción del delito en la relación acción u omisión detectada en la descripción típica o a la realización de diversas formas en el concursos delictivo, a la operación natural de la concatenación de acciones ilícitas, para lograr un eje de poder criminal con varios negocios a partir de un delitos base, por ejemplo; un robo de auto móvil significa a la vez: tráfico de drogas, tráfico de personas, homicidio y venta de auto partes.

Fragmentar el delito significa crear estructuras criminales bajo el esquema de operación o sub operación delictiva. De igual manera las formas intimidantes de actuar o dominar espacios geográficos sin límites por parte de los criminales han generado una escalada de violencia cotidiana donde pocos espacios son seguros.

México ha pasado los últimos 20 años probando modelos policiales y estrategias de combate al delito con éxitos pírricos. El delito se ha dispersado de tal forma que los esquemas de la prevención

11 *Cfr.* "Califica AMLO como "narco gobierno" y "gobierno mafioso" a sus antecesores". *Aristegui Noticias* https://aristeguinoticias.com/1610/mexico/califica-amlo-como-narcogobierno-y-gobierno-mafioso-a-sus-antecesores/ Consultado: 5 enero del 2020.

general negativa y la prevención social de la violencia se van mostrando poco útiles, de forma particular en las zonas marginadas del desarrollo social y económico.

Los delitos han dejado de ser o comprenderse de forma aislada a la voluntad del sujeto bajo ciertas presiones sociales. Hoy la etiología delictiva surge en gran medida al seno de las familias criminales, en los procesos de dominación vecinal, en las escuelas, los pueblos, las zonas comerciales las carreteras y por supuesto en el gobierno mismo. El delincuente se mueve de un lugar a otro con gran velocidad y se transforma dependiendo el medio (lugar y bases que lo gestan) y las circunstancias que motivan su transformación y operación no encuentran límites.

Es por ello que las cifras oficiales del control delictivo nos dan realidades meramente circunstanciales o momentáneas. Para poder combatir la nueva incidencia delictiva y sus procesos de fragmentación la autoridad depende cada día más de la tecnología como forma de acotar los proceso delictivos y tener una mejor estrategia de combate reactivo y preventivo al crimen, local y organizado.

La movilidad del fenómeno del delito es natural a las estrategias de presencia institucional de la policía lo que va generando el cambio en la realización del delitos y los patrones de ejecución del mismo e incluso el abandono parcial de la actividad para cambiarla por otra; en otros casos, la vigilancia territorial del delincuente usando soplones, halcones y mirones que facilitan el escape de capos y el ocultamiento de las actividades ilícitas.

Los criminales hoy basan su movilidad a través de predios y túneles, se esfuman de la autoridad de muchas formas, complicando el combate efectivo al delito. Es por esto que cada vez más las estrategias de seguridad y control de delito van incorporando el uso de la tecnología para poder cumplir sus tareas e incluso se han ido tecnificando las políticas criminales para poder preservar el orden e imponer un Estado fuerte. La vigilancia y el procesamiento de información respecto de las distintas formas del comportamiento

criminal se van volviendo urgentes e inaplazables.

La idea central de las políticas de tecnificación y procesamiento de información para el control de delitos observa 6 ejes: primero, control territorial; segundo, control de movilidad delictiva; tercero, identificación silenciosa; cuarto, rastreo y visualización preventiva; quinto, fijación de imágenes en tiempo real y sexto; procesamiento de información y generación de inteligencia. Dichos ejes le dan al Estado el factor sigilo y mayor precisión para evitar los controles territoriales que tienen los delincuentes y de los que ya hemos hablado.

Una de las estrategias que encierra estos seis ejes es la inteligencia geoespacial, ya que existe otras estrategias y herramientas tecnológicas que pueden tener una o varias de las características enunciadas.

La aplicación de herramientas tecnológicas a las estrategias de política criminal de combate y prevención de delitos es costosa pero evita enfrentamientos físicos, da el factor sorpresa y pude monitorear cada movimiento reduciendo significativamente la fuga de información. El uso de tecnologías como la inteligencia geoespacial ha sido probada en campos militares y puede ser de gran utilidad para controlar ciertos delitos y generar formas preventivas.

Así entonces veamos en que consiste la inteligencia geoespacial y cuál es su relación específica con la política criminal.

III. INTELIGENCIA GEOESPACIAL Y SU VÍNCULO CON POLÍTICA CRIMINAL

La Inteligencia Geoespacial, abreviada como GEOINT[12], es aquella disciplina que realiza la explotación y el análisis de imágenes, datos e información del espacio terrestre. Se encarga principalmente de describir, evaluar y visualizar aquellas representaciones o ca-

12 En inglés llamada: "*Geospatial Intelligence*", se desarrolló en Estados Unidos y actualmente, se busca replicar en el sistema de seguridad internacional.

racterísticas físicas, geográficamente referenciadas de la tierra. Su participación en el ciclo de inteligencia es de suma importancia, ya que esta disciplina se realiza y se encuentra durante la etapa de colecta de información.[13]

El término de Inteligencia Geoespacial fue presentado por el General James R. *Clapper,* quien fue el ex director de la Agencia Nacional de Imágenes y Cartografía (NIMA)[14] de Estados Unidos, *Clapper* se encargó de adoctrinar a la organización, desarrollando líderes y enseñarles cómo obtener este material para fines de apoyo a la nación.[15]

Los principales elementos para lograr un producto sobre esta disciplina son las imágenes, la Inteligencia en Imágenes (IMINT)[16] y la Información Geoespacial. Se trata de explicar de forma propia y útil la representación de forma natural o artificial de cualquier cosa, cuyo objeto es relacionarlas a datos meramente posicionales y a productos de reconocimiento basado en espacios de interés aplicando la inteligencia.

Para la colecta de información es necesario el uso de satélites, esto varía con su naturaleza y su utilización. Existen satélites que se encargan de obtener información de acuerdo con la necesidad y los intereses nacionales de un país. El acceso a estos satélites se dá mediante convenios entre naciones, por medio de sus agencias o centros de investigación para la seguridad nacional.

---

13 *Cfr. Department of the Army*. "*Geospatial Intelligence Handbook*". Washington D.C. United States of America: Department of the Army, p.11, 2011. Consultado: 7 agosto del 2020

14 En 2003, se transforma en la Agencia Nacional de Inteligencia Geoespacial (NGA), actualmente esta agencia realiza GEOINT para el Departamento de Defensa de los Estados Unidos y administra el Sistema Nacional de Inteligencia Geoespacial.

15 *Cfr. Kovarík*, V. "*Understanding the Role of Geographic Data and Processes in Geospatial Intelligence*". Conferencia Científica y Técnica Internacional, Bratislava, publicación elaborada para la Universidad de Defensa, p.1-7, 2012. Consultado: 14 abril del 2020.

16 En inglés llamada: "*Imagery Intelligence*".

Durante la colecta satelital, se utilizan sensores y radares que le dan mejor calidad a las imágenes y detalles de las zonas.[17]

Una constelación de satélites puede proveer información exacta. Se debe contar con información precisa sobre latitud y longitud[18], los kilómetros de radio que se abarcan, si requieren o no un polígono, el tipo de sensor[19], el día de inicio y el día final de visualización para la captura de imágenes, el huso horario de la zona, su rango de prioridad para su registro y petición, la fecha de entrega, especificaciones sobre el área de la agencia o centro que está requiriendo esta información, mediante peticiones a sus especialistas.

Su siguiente componente es la Inteligencia de Imágenes (IMINT) que se deriva de la interpretación o el análisis de imágenes obtenidas por sistemas de reconocimiento producidas por plataformas terrestres, marítimas y/o aéreas con o sin ayuda de una persona; es indispensable esta disciplina como herramienta para determinar información necesaria para la toma de decisiones.

Estos elementos funcionan para identificar la locación geográfica exacta y las características naturales que presenta la zona específica, así como sus límites y fronteras construidas en la Tierra. Esto incluye estadísticas e información derivada de la teledetección, mapeos y el uso de tecnologías relacionados con sensores remotos, cartografía, topografía y datos geodésicos.

Es importante relacionar las capas de datos dentro de esta otra disciplina porque va acompañada de la información espacial o geoespacial. Estas capas proporcionan detalles para uso civil, policial, geoespacial, militar, entre otros. En un inicio, la información geoespacial era un recurso estratégico para el cumplimiento de las misiones que las Fuerzas Armadas encomendadas tanto en territo-

---

17 *Cfr. United States Navy. Geospatial Intelligence in Joint Operations. Joint Publication*, 2(03), 2007,p.15-17, 2017. Consultado: 23 abril del 2020.

18 Incluyendo si es hacía el Norte o Sur y si es hacia el Este u Oeste.

19 El tipo de sensor viene señalado en los formularios para la creación de las constelaciones satelitales, suelen utilizar el *Sensor STR HD Image*, debido a que tiene una alta calidad a nivel de telemetría y la resolución será excelente.

rio nacional como en el exterior en algunos países pertenecientes a la OTAN.[20]

La información espacial es reflejada en mapas o croquis, acompañada con gráficas y estadísticas que permiten entenderse en su totalidad para todas las personas que debían tomar decisiones. Actualmente, se utilizan los Sistemas de Información Geográfica[21], que fueron diseñados para trabajar con datos referenciados mediante coordenadas espaciales o geográficas, que tienen dos elementos fundamentales que son la tecnología y la información, enriqueciendo todo proceso en una investigación.[22]

Aunque los SIG principalmente son herramientas de uso territorial, son destinados a apoyar la toma de decisiones y para visualizar espacialmente las nuevas tendencias en el desarrollo de las regiones.[23]

Hablando de Política Criminal, existen grupos que se dedican a promover delitos de alto impacto, su principal motivador es el dinero, su cobro puede ser a nivel de criptomonedas y el resultado se refleja en el mundo material y la comisión de otros delitos como lo son, los homicidios, secuestros, robos, tráfico de armas, tráfico de personas, tráfico de flora y fauna, tráfico de órganos; algunos de

20 *Cfr.* Bernaldo de Quirós, J. "*La Política Geoespacial en el Ministerio de Defensa*". España,Instituto Español de Estudios Estratégicos, 2011, p.3. Consultado: 22 octubre del 2018

21 *Softwares* de visualización de datos e infraestructuras geoespaciales. La infraestructura de información espacial en la Unión Europea, llamada *"Infrastructure for Spatial Information in Europe"* (INSPIRE), tiene como objetivo poner a disposición órganos responsables en la toma de decisiones o aplicación de políticas comunitarias, datos espaciales abundantes y fiables. Se encargan de crear servicios destinados a mejorar la accesibilidad e interoperabilidad de los datos. En México tenemos a INEGI y la UNAM que se encargan de crear bases de datos con información clave para los estudios poblacionales.

22 *Cfr.* Olaya, V. "*Sistemas de Información Geográfica*". España: CreateSpace Independent Publishing Platform (Amazon), p7-8, 2014. Consultado: 28 septiembre del 2018.

23 *Cfr.* Rodrigo Hidalgo, M.L. "*Las tecnologías de información geográfica y su aplicación al análisis urbano. El caso del estudio de los espacios residenciales cerrados en las áreas metropolitanas de Santiago y Valparaíso*". Revista Electrónica de Geografía y Ciencias Sociales. *Universitat* de Barcelona. España, 2004. Véase en: http://www.ub.edu/geocrit/sn/sn-170-31.htm junio 2020

estos delitos impactan a la población vulnerable, en delitos como la pornografía infantil, explotación y turismo sexual, delitos lesivos para las víctimas del delito y la sociedad.

Estos delitos, en nuestro país, son de alta peligrosidad, muy difícil de encontrar o identificar si no existiera la policía cibernética. Es muy difícil de comprobar porque las redes que manejan dentro de todo este tráfico, producción o difusión de material sensible, podemos decir qué tecnológicamente hablando, han avanzado e incrementado barreras que pueden engañar a un policía.

Aquí la importancia para la política criminal, el derecho penal y dentro de estas disciplinas existe el uso de la Inteligencia Criminal, la Inteligencia Geoespacial, la vigilancia y el monitoreo, todas estas herramientas de análisis se vuelven esenciales para la identificación de factores terrestres, marítimos, aéreos y del ciberespacio que puedan vulnerar la seguridad nacional de un Estado.

El uso de la inteligencia geoespacial es justificable siempre y cuando los objetivos estén limitados para combatir a los miembros de la delincuencia organizada[24] tanto nacional como transnacional[25]. Sería justificado para monitorear bandas locales. Incluso cuando se ve enfocado directamente a misiones del mantenimiento de paz, conflictos bélicos internacionales y fronterizos, o generen un ataque inminente a un Estado. Debemos recordar, por ejemplo, en México en los últimos años –de 2018 a 2020- los fenómenos migratorios masivos ha provocado que se oculta el delito, por una cifra negra impresionante, debido a que los migrantes suelen ser víctimas como elementos de reclutamiento a bandas criminales. Observar estos movimientos, sus rutas, sus enclaves dentro del territorio, su fusión

24 En México, la delincuencia organizada ha evolucionado durante el paso del tiempo, aunque siguen controlando territorios, ya no buscan eliminar a ciertos objetivos. Un ejemplo claro para provocar un "respeto" se daba entre cárteles en los años 80's y 90's. Los grandes cárteles del narcotráfico han logrado desarrollar nuevas estrategias para obtener mayor influencia en el territorio, fortaleciendo estrategias entre los ciudadanos, sus miembros, mandos municipales con alianzas y aprovechando el suelo que se tiene en cada región.

25 Aquí se derivan muchos de los delitos que deben ser estudiados en nuestro país.

con grupos locales, la cantidad de migrantes y su dispersión pueden dar información para la prevención y ayuda a estas personas vulnerables pero también para tener procesamiento de información clave para perseguir delincuentes.

En la inteligencia se debe identificar un potencial agresor o ya previamente conocido, sea un individuo, célula delictiva, grupo ideológico o Estado, entre otros.

Los agresores o delincuentes organizados suelen estudiar las dimensiones territoriales de la zona que van a atacar o en la que generarán impactos negativos (daños o amenazas); por ellos la inteligencia permitirá generar procesos anticipación o de reacciones preventivas.

Es por eso que el uso de la inteligencia, debe ser considerado esencialmente preventivo para advertir la probabilidad de un suceso, con ello se hará factible una intervención primaria para después aplicar las leyes y políticas para sancionar estas conductas delictivas que se pueden convertir en una amenaza inminente o tenga un agresor en específico en el uso para la defensa de un Estado a nivel seguridad pública y seguridad nacional.

Los pilares importantes para la colecta de información inician con la confidencialidad, esto significa que se debe mantener en un estatus de secreto la información sensible, como la obtención de imágenes geoespaciales de una zona específica. Inclusive se podría considerar un uso restringido que significa que personal especialista pueda tener acceso, estudio y análisis de esta información.

Al verificar la identidad de los agentes implicados en los estudios -como lo son personas claves dentro miembros de alguna asociación u organización delictiva, instituciones o Estados- podrá desarrollarse una red que podrá contribuir a un caso importante para una nación. La inteligencia geoespacial funciona relacionando el monitoreo y vigilancia, como factor primario para lograr cumplir estándares de eficacia, los que conlleva a la veracidad e integridad de la información de acuerdo con las fuentes; esto enmarcará la continuidad con el apoyo de la policía de investigación.

Con ayuda de la Criminología Ambiental[26], como parte de una estrategia para la Seguridad Ciudadana, se apoyará a las instituciones que se encarguen de la colecta de información, brindando una mejora a las instituciones policiales. Así se podrá conocer el entorno o contexto para identificar posibles focos rojos que puedan vulnerar a la población e intentar prevenir el delito a partir de influencias situacionales.

En la dimensión terrestre, es importante mencionar los grandes mapas creados por especialistas en seguridad, que visualizan las grandes extensiones estatales que tienen los grupos de la delincuencia organizada como sus brazos armados. La mayoría de los especialistas se han enfocado en mantener estos datos actualizados para identificar patrones de comportamientos a lo largo del territorio mexicano.

También se involucra a especialistas y personal encargado en estudiar el diseño de las calles, manzanas, localidades, entidades y áreas metropolitanas (topógrafos) para la toma de mejores decisiones con el fin de mejorar la calidad de vida de la población.

Algunas de las estrategias derivadas de la inteligencia geoespacial tienden a dar información aplicable en la criminología situacional ambiental, desarrollándose así estrategias de control de recuperación de espacios, diseño de áreas seguras y la colocación de tecnología que inhiba al delincuente, todo esto desde cosas sencillas como alarmas, sensores, luces temporizadas o tecnología que hace invisible de movimiento, sensores de temperatura, corte de señales para aparatos de comunicación, intercepción de registros de datos etc.

También se aplica a la arquitectura de control preventivo creando nuevos espacios de recreación como parques o centros culturales, evitar que existan lugares que promuevan a la delincuencia poder llegar y allanar ese espacio para usos ilícitos, etc. El uso de estrategias en la criminología ambiental permite con la incorpo-

26 Estudia el espacio o lugar y el momento en el que se ha cometido algún hecho delictivo.

ración y cooperación de la sociedad con las instituciones públicas para implementar programas para reducir la cantidad de delitos de zonas con alto índice de delincuencia y promover la cultura de seguridad a toda la población.

Parece ser todo esto muy utópico debido a que no se vive en un país donde existe una repartición favorable de la riqueza, donde los recursos cada vez escasean más y el desempleo sigue aumentando generando factores de proclividad delictiva más aún en situaciones de urgencia social como lo es la pandemia COVID de este año 2020, que favorece la movilidad del delitos haciendo suyas cada oportunidad de desconcierto y vulnerabilidad social.

Antes solo se evaluaban zonas criminógenas pequeñas, ahora los escenarios son las grandes ciudades. Se debe evitar situaciones de incertidumbre y sensación de inseguridad para los ciudadanos, por lo que es indispensable abatir el miedo al delito y cambiar la percepción real de inseguridad, utilizando la inteligencia y la tecnología como herramientas para una mejora en la política criminal.

La tecnología es un factor importante para identificar vulnerabilidades de un actor (posible activo). El delincuente también usa la tecnología y busca ir un paso delante de la policía y la ciudadanía, es por ello vital hacer un uso preciso y continuo de la inteligencia y sus aplicaciones.

Así entonces, la Inteligencia Geoespacial se encargará de identificar cada territorio antes, durante y después de cada conflicto. Elaborará planes para guiar a los elementos (reactivos-preventivos) a lugares estratégicos sin que peligren sus vidas, monitoreándolos. Es importante recordar que los miembros de la comunidad de inteligencia deben cumplir la ley, y conducirse por órdenes judiciales.[27]

En el caso de que exista un conflicto armado, los especialistas en la materia, podrían establecer zonas de protección para la pobla-

---

27 *Cfr. Lowenthal, Mark M.* "*Intelligence: From Secrets to Policy*". Estados Unidos. Editorial. CQ PRESS & SAGE, chap. 13, 2015, p.413. Amazon *(Kindle)*. Consultado: 10 noviembre del 2018

ción civil quienes no tienen que estar en el campo las zonas de conflicto. El impacto ético debe cubrir una necesidad humana básica, respecto de daños reversibles e irreversibles, planteando alternativas beneficiosas para involucrados y dañados. Se deben minimizar los impactos negativos ambientales en su ejecución. [28]

La tecnología muchas veces es cuestionada, pero hay acuerdos internacionales[29] que limitan las acciones como la Convención de Ginebra, muchas ocasiones ha sido violada por países argumentando que lo hicieron por su supervivencia, seguridad y la protección de su territorio.[30]

IV. APLICACIONES ADICIONALES: INTELIGENCIA-POLÍTICA CRIMINAL

Como es sabido, la política criminal dentro del derecho penal se encarga de estudiar las causas y el análisis del delito, el delincuente y su personalidad, la víctima, las sanciones, medidas de seguridad, la construcción y control del delito, la prevención de la violencia y las reacciones sociales ante el crimen.

Es por eso importante destacar algunas formas de utilidad de los productos de la inteligencias en las distintas áreas de incidencia de la política criminal a partir de su definición.

---

28 *Cfr.* Byrne, E.. "Making Drones to Kill Civilians: Is it Ethical?". Springer Science+-Business Media, Dordrecht.America. 2015,p.7. . Véase en: https://scholarworks.iupui.edu/bitstream/handle/1805/9741/Byrne_2015_making.pdf?sequence=1, Consultado 18 septiembre del 2018.

29 Aquí entra el concepto de utilidad de la fuerza, debe ser lícita y haber sido plasmado en acuerdos por Naciones Unidas. Es irrenunciable esta obligación ya que tiene una validez universal, afecta todo el mundo, no debe ser ignorada, se debe obligar el cumplimiento de estos acuerdos. Sus excepciones del uso de la fuerza contemplan la legítima defensa y la acción coercitiva, si un consejo de seguridad nacional toma la decisión de defenderse, es válida, siempre y cuando haya una amenaza o quebrantamiento que impide que se respete y mantenga la paz.

30 *Cfr. Los Convenios de Ginebra de 1949 y sus Protocolos adicionales*. Comité Internacional de la Cruz Roja. Ginebra, Suiza. 2010. Consultado 14 octubre del 2018.

Primero:

La percepción del crimen impacta en la vida de los individuos. El crimen es medido con estadísticas oficiales del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública; esta institución se encarga de estudiar, medir y evaluar los delitos en materia de fuero federal y fuero común.

En función de esto y para esto la inteligencia puede favorecer el mapeo de zonas de riesgo en tiempo real consecuentemente establecer zonas de vigilancia, movilidad de los posibles delincuentes, áreas de influencia criminal, tráfico de personas y mercancías, detección de cultivos y caminos clandestinos.

La importancia aquí es que la inteligencia debe asociarse y contribuir a la generación de esta estadística y no sólo a la recolección de la información día con día en datos estadísticos.

Segundo:

En el Sistema de Justicia Criminal tendríamos una mejor organización para la prevenir, investigar y analizar información que se traduzca en datos de prueba para de las carpetas de investigación, lo que permitiría dirigir las investigaciones de forma eficiente y contundente de forma particular contra delincuencia organizada y delincuencia trasnacional.

La idea es que la probabilidad de recibir una sanción penal se traduce en probabilidad de ser arrestado, procesado, acusado, juzgado y condenado de forma real y contundente. Al combinar las leyes y/o actividades contribuirán para reducir al mínimo los posibles costos de la inseguridad y del control del crimen para medidas relevantes de disuasión, aspectos operativos, presupuestales y organizacionales. Consecuentemente mejorará la rehabilitación como tratamiento para reformar o cambio valores.[31]

---

31 *Cfr. Hassemer Winfried*-Muñoz Conde, Francisco. *Introducción a la Criminología y a la Política Criminal*. Tirant Lo Blanch. España, Valencia, 2012. Consultado 22 septiembre del 2018.

Tercero:

La tasa de delitos elevada produce un miedo alto en los ciudadanos, este se mide de acuerdo con la preocupación de la víctima, las denuncias realizadas ante las fiscalías, la presunta ocurrencia de delitos registrados en carpetas de investigación, la percepción del crimen en una comunidad y aquellas posibilidades de convertirte en víctima.

El Estado es el responsable de garantizar seguridad y procuración de justicia, radica en legitimar políticas de seguridad. Al comprender los patrones delictivos dentro de un espacio urbano, los delincuentes pueden tener o no un trabajo, familia estable, realizar actividades de recreación y cometer ilícitos alrededor de espacios cercanos a su residencia.

La delincuencia juvenil en áreas urbanas es identificada por la creación de mapas que muestra la desorganización social, las imágenes espaciales sobre algunas calles peligrosas donde suelen desarrollarse estos grupos delictivos. La falta de una estructura familiar implica que los menores incursionen en estas actividades delictivas.

La creación de los mapas del crimen, enfocados en *hot-spots* como estudio del área que supera los eventos delictivos. Los estudios geográficos de la delincuencia empiezan relacionando ese espacio físico, la mayor parte del tiempo en áreas y perímetros peligrosos donde se debe implementar mayor seguridad policial[32]. Como el estudio de perfil geográfico relacionado a la inteligencia geoespacial para su análisis de investigación criminal acercándose a la posible zona donde actúa el delincuente.

La Ley General para la Prevención Social de la Violencia y la Delincuencia considera que la prevención situacional o criminología ambiental, al buscar restringir las posibilidades de cometer

32 La Interpol realiza informes sobre criminales con ayuda a los organismos encargados de la aplicación de leyes nacionales en elaboración de políticas para la toma de decisiones haciendo frente a los desafíos que pueden establecer prioridades en la investigación, en operativos y nuevas estrategias.

infracciones y aumentar el esfuerzo del delincuente. La prevención social del delito buscando proporcionar aquellas condiciones sociales, educativas, culturales para el bienestar y evitar el desarrollo de factores de riesgo. La prevención del crimen a nivel local o comunitaria, modificando las condiciones locales que influyen en la delincuencia, en la victimización y en la inseguridad.[33]

Cuarto:

Las principales fuentes de información para la mejora de una política criminal son: censos de población, encuestas nacionales sobre niños y jóvenes, salud pública y antecedentes sobre lesiones, accidentes y muertes violentas, consumo de drogas, el uso de suelo, condiciones, servicios ambientales, servicios penitenciarios y de justicia sobre delincuentes, características, modalidades de condenas, menores recluidos, tipos de tratamientos, tasas de reincidencia, observatorios de criminalidad al recoger y evaluar información sobre delitos, problemas sociales y diagnósticos de seguridad.

Se debe crear una asociación directa y coordinada entre fuerzas federales y locales.

La adecuada coordinación con distintas instituciones de la seguridad pública y fiscalías especializadas, se dará el seguimiento de investigaciones sobre infractores del delito y brindar mayor seguridad a las familias, generando un diagnóstico participativo de la comunidad. La investigación criminal está centrada en información real, que permita no tener como pilar de acción o justificación la denuncia como medida falaz de intervención de los cuerpos del Estado sino información clasificada que deberá de tener valor probatorio para que el trabajo policial sea legal y legítimo.

El trabajo de inteligencia si es un control duro pero debe de ser así porque es la manera real de posicionar al Estado fuerza impactando con tecnología de punta al crimen y sus áreas de influencia.

---

33 *Cfr.* "*Ley General para la Prevención Social de la Violencia y la Delincuencia*". Cámara de Diputados del Honorable Congreso de la Unión México: DOF, 2012. Véase en http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPSVD.pdf Fecha de Consulta Agosto de 2020

Quinto:

Información es poder. La inteligencia geoespacial aplicada a la política criminal pude generar posicionamiento del Estado evitando fugas de información bajo un estricto cerco de manejo de información y aplicación de los mismos. La inteligencia a distancia y a través de satélites debe de vulnerar a la mayoría de los grupos criminales que no cuentan con ese poder tecnológico y al mismo tiempo develara el uso que el Estado haga de ella evitando abusos de poder.

La inteligencia y el procesamiento de datos a distancia controlarían reclusorios, carreteras, aeropuertos clandestinos y mucho más. Su aplicación como se dijo en un principio requería para no ser utópica de un convencimiento real para posicionar en Estado fuera del control mafioso, deberá de cambiar la historia (como la que iniciamos éste artículo) dando al ciudadano el poder real de decidir si los aparatos represivos del Estado sirven a la democracia ciudadana o al poder político corrupto; desde esa perspectiva se develaría si los fiscales en realidad traban en *pro* de sus propios cometidos constitucionales con información confiable, precisa, no contaminada que se traduzca en procesos contundentes y apegados a derecho.

Sexto:

La información geoespacial en la política criminal clarificaría las dinámicas sociales que de forma no convencional se den en determinadas geografías previendo procesos violentos o atípicos que puedan transformarse en delitos por ejemplo, grupos guerrilleros, movimiento de narcotraficantes, invasiones de predios etcétera.

Aplicaciones pueden ser muchas. Se han mencionado algunas que son las más comunes y que podrían ser objeto de diseño de políticas criminales y de seguridad nacional y pública. La inteligencia es información aplicada con fines benéficos y ya debería de ser parte en una sociedad cada día más tecnificada.

V. REFERENCIAS INTERNACIONALES E INSTITUCIONES MEXICANAS, USO MASIVOS

Como principal referencia internacional tenemos a las Naciones Unidas, dentro de esta organización existe una oficina responsable de promover la cooperación internacional, es la Oficina de las Naciones Unidas para Asuntos del Espacio Ultraterreste (UNOOSA[34]), la cual se encuentra en la Oficina de las Naciones Unidas en Viena, Austria; esta oficina interviene en los usos pacíficos del espacio exterior.[35]

La UNOOSA es la responsable de implementar en virtud de Derecho Internacional del Espacio, para mantener el registro de objetos lanzados al espacio exterior por las Naciones Unidas, prepara y distribuir informes, estudios y publicaciones sobre diversos campos de las aplicaciones de la ciencia y la tecnología espaciales y el derecho internacional del espacio.

¿Por qué relacionar el espacio exterior o ultraterrestre? Porque, gracias al Derecho Internacional, tiene sentido el uso de constelaciones satelitales o peticiones de zonas geográficas exclusivamente para uso de investigación y brindar ayuda en tiempo casi real a naciones con alguna catástrofe natural, nuclear o provocado por el hombre.

Lo interesante de la oficina de la UNOOSA es que mantiene una línea telefónica directa de 24 horas como punto focal de las Naciones Unidas para solicitudes de imágenes satelitales durante desastres y administra la Plataforma de las Naciones Unidas para la información espacial para la gestión y respuesta de emergencia.

¿Cómo se puede obtener la información geoespacial de manera internacional? Bueno, aunque los convenios y peticiones son necesarias, existe la Unión Internacional de Telecomunicaciones (UIT), la cual también perteneciente a las Naciones Unidas.

---

34 En inglés: "*United Nations Office for Outer Space Affairs*". El espacio exterio

35 *United Nations Office for Outer Space Affairs*. "*Roles and Responsibilities*. About us. United Nations ». Viena, Austria 2015. Véase en: http://www.unoosa.org/oosa/en/aboutus/roles-responsibilities.html Consultado : Agosto 2020.

Un dato histórico sobre la UIT es que, durante la resolución de la Asamblea General de 1962, se aprobó que las Naciones Unidas deberán establecer principios legales que regirán las actividades en la exploración y uso del espacio exterior, por el bien de la humanidad y en el desarrollo de las naciones. Dentro de los principios establecidos, cada país debería ser internacionalmente responsable de sus actividades nacionales realizadas, ya sea por organizaciones gubernamentales o no gubernamentales[36].

Dentro de la Ley Federal de Telecomunicaciones y Radiodifusión, se menciona la órbita satelital, que es considerada como la trayectoria que recorre una estación espacial alrededor de la Tierra. Diversos incisos hablan sobre que se debe administrar y vigilar, el uso eficiente de la capacidad satelital propia, ya sea concesionada, adquirida o establecida como reserva y a favor del Estado. Así como establecer y procurar políticas que promuevan tanto la capacidad y la disponibilidad de servicios satelitales para redes de Seguridad Nacional para apoyar necesidades, objetivos y fines del Gobierno Federal.[37]

En México, la Secretaría de Telecomunicaciones y Transportes es la encargada de vigilar el uso de los satélites, y debe observar si se contribuye con estos para mantener a nuestro país protegido, brindar apoyo a protección civil, ayuda humanitaria y en operaciones de seguridad nacional durante sus tareas de inteligencia, seguridad, toma de decisiones e implementación de políticas nacionales en materia satelital.[38]

---

36 Las actividades que las entidades no gubernamentales pretenden llevar a cabo deben estar autorizadas y supervisado por el Estado interesado. Si el Estado decide explorar o utilizar este espacio, se guiará por el principio de la cooperación y asistencia mutua.

37 *Ley Federal de Telecomunicaciones y Radiodifusión.* México, Cámara de Diputados del Honorable Congreso de la Unión. México: DOF. 2014, Véase en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_150618.pdf

38 Secretaría de Comunicaciones y Transportes. *Política Satelital de México*. México, Gabinete Legal del presidente de México. 2017, Véase en: http://sct.gob.mx/fileadmin/DireccionesGrales/Comunicaciones/2017-consulta-publica-politica-sate-

Aquí es importante mencionar a la Agencia Espacial Mexicana, se encarga de promover y desarrollar una cultura de interés espacial para la adecuación de nuevas investigaciones y promociones de información relevante para la explotación de la seguridad nacional a nivel gubernamental.

Esta Agencia depende de la Secretaría de Comunicaciones y Transportes, la cual forma parte de una red internacional de centros y agencias espaciales, que trabajan en conjunto para colaborar en la solución de problemas a nivel global. Muy pocas personas conocen los grandes avances que ha tenido desde su creación, el impulsar esta agencia puede ser el acierto más grande en temas de seguridad espacial y geoespacial a nivel nacional.

La agencia realiza diversos congresos con enfoque en las debilidades de los territorios para el uso de tecnología que permita identificarlas. También y gracias a los convenios, las misiones entre países pueden alcanzar éxito en sus diversos usos. El contacto global es importante para poder conocer que es lo que se está realizando en otro país positivamente para su población e intereses nacionales.

Existen convenios que intensifican las relaciones entre las agencias y los centros a nivel mundial, así como su cooperación inmediata. El nivel de compromiso es tan extenso que no importa el tiempo que se le dedique a una petición entre agencias, la interoperatibilidad que se tiene es excelente y eficaz.[39]

Un ejemplo muy claro es la obtención de información geográfica, geofísica y geoambiental de los sistemas de posicionamiento de la constelación LANDSAT, creado en Estados Unidos para el monitoreo de recursos terrestres. Actualmente LANDSAT-8 recopila imágenes de todo el planeta cada 16 días, esta constelación es operada por la Administración Nacional de Aeronáutica y del Espacio (NASA), todo esto se ve relacionado con la política criminal, si su-

---

lital.pdf Fecha de consulta: Agosto del 2020

39 Santamaría Roa, Karla. *Testimonio propio, experimentado durante sus prácticas profesionales en la Agencia Espacial Mexicana en 2019*. (responsabilidad de quién cita).

cede un escenario donde una banda del crimen organizado actúan en zonas específicas, al poder ser identificados en sus movimientos y los cambios que realizan en sus operaciones en cada momento. Los satélites captan imágenes en tiempo real de ángulos distintos de la tierra cada día, por lo que, sería una herramienta para la identificación de emergencias en zonas vulnerables y su evolución.[40]

La Inteligencia Geoespacial no se considera un producto de inteligencia en México, debido a que solo se presenta en la etapa de colecta de información, funge como herramienta para identificar posibles riesgos u amenazas del objeto de estudio.

El antiguo Centro de Investigación y Seguridad Nacional (CISEN), ahora El Centro Nacional de Inteligencia (CNI), era el lugar encargado de colectar información geoespacial para un mejor análisis geográfico. Esto se puede leer dentro de la Ley de Seguridad Nacional, refiriéndose a: "*operar la tecnología de comunicaciones especializadas*", fundamentado dentro del artículo 19, inciso IX del Capítulo II, esto se puede utilizar los satélites como herramientas para la política criminal en el monitoreo de zonas estratégicas o focos rojos dentro de la criminología ambiental, aplicado a un lugar geográfico[41].

Dentro de la División Científica de la Policía Federal, existe el área de Innovación Tecnológica, donde construyen y utilizan drones para el monitoreo y vigilancia de zonas consideradas como foco rojo y de difícil acceso, obteniendo datos geoespaciales como imágenes y coordenadas precisas del lugar en conflicto. Todos estos datos son procesados para el área de División de Inteligencia, quienes se encargan de analizar y realizar el producto de los fenómenos geoespaciales.[42]

---

40 La producción y la comercialización de las imágenes depende del Servicio Geológico de los Estados Unidos (USGS).

41 *Ley de Seguridad Nacional*. México, Cámara de Diputados del Honorable Congreso de la Unión México: DOF. 2015. Véase en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf fecha de consulta: marzo 2020

42 Hecho que consta por ser verificado con la visita realizada a instalaciones de Poli-

La Policía Federal se consideró el principal usuario de drones en el año de 2015. Las actividades de narcotráfico incluyen la producción de droga, cocaína y marihuana, así como su introducción a los Estados Unidos, e incluyendo el contrabando de armas hacia México y América Central. Han sido empleados con éxito en la conducción de operaciones de vigilancia en apoyo de acciones lanzadas por la Policía Federal y el Ejército Mexicano contra células del narcotráfico en Ciudad Juárez, Culiacán y Tijuana al norte de nuestro país.[43]

La inteligencia geoespacial en las fuerzas armadas es obtenida por la Fuerza Aérea Mexicana, la cual dependiente de la Secretaría de la Defensa Nacional (SEDENA), es una herramienta que es sumamente útil durante el proceso de análisis a la comunidad de inteligencia militar, mediante el reconocimiento aéreo y su coordinación con satélites americanos, permitiendo una mayor claridad en la identificación de cultivos de amapola, el cuidado de las fronteras y puertos de nuestro país.[44]

El territorio marítimo y aéreo han sido monopolizados por las fuerzas armadas, su dominio es tan extenso que los perímetros que manejan están a lo largo de toda la República Mexicana, por lo que brindan una mayor percepción de seguridad que si una autoridad policial permaneciera en estos puntos de reacción para defender un territorio.

Los reconocimientos aéreos realizados por las fuerzas armadas han permitido denotar y modificar en los datos geoespaciales, extensiones de tierra dominadas por grupos de la delincuencia para el uso y cultivo del cannabis, encontrar casas de seguridad o la identificación de objetivos para su detención.

---

cía Federal en la División Científica 19 de octubre de 2018. Policía Federal. México.

43 Higuera, J.. *"Vehículos Aéreos No-tripulados: El escenario latinoamericano"*. México, Tecnología Militar, Volumen III. 2013. P 2

44 Información obtenida de: *Conferencia de Inteligencia Estratégica*. 10 de octubre de 2018. Sub jefatura de Inteligencia Militar; Estado Mayor de la Defensa Nacional. Universidad Anáhuac México Campus Norte. México.

En el ámbito civil, el Consejo Nacional de Ciencia y Tecnología (CONACYT) apoya al actual Centro de Investigación en Ciencias de Información Geoespacial y el Laboratorio Nacional de Geointeligencia, quienes realizan modelos de análisis espacial y de territorialidad, cuentan con plataformas de servicios para investigación, siendo meramente académico.[45]

La Universidad Nacional Autónoma de México (UNAM) desarrolla visualizadores para el uso de la Protección Civil, programas de Licenciatura, Maestría y Doctorado, así como reciben el apoyo directo del Instituto Nacional de Estadística y Geografía (INEGI), quienes cuentan con sus propios aviones para el debido reconocimiento aéreo y obtención de imágenes geoespaciales.[46]

La recolección puede considerarse un problema, pero a la vez una ventaja, el hecho de que sea regional, su nivel de colecta es efectiva y más segmentada dentro del país. Esta recolección relaciona todo el aspecto cartográfico. El problema de los servidores o buscadores internacionales es que existen zonas donde no se logra apreciar debidamente las limitaciones como lo son las bases aéreas o zonas de uso exclusivo de ejércitos mundiales y su resguardo de armas de destrucción masivas.

Dentro de la experiencia de la Federación Internacional de Futbol Asociado (FIFA), podemos encontrar que con apoyo de agencias de Inteligencia y la cooperación de policías internacionales, se han apoyado antes y durante eventos masivos, apegado a la legalidad para sancionar conductas ilícitas dentro del recinto deportivo.[47]

En el mundial de Sudáfrica, contaron con la participación de

---

45 Ellos colaboran con el Centro de Investigación en Matemáticas y el Centro de Investigación en Geografía y Geomática.

46 *Cfr.* INEGI en México es la Infraestructura de Datos Espaciales nacional, como lo es INSPIRE en España y la Unión Europea.

47 Implementando el uso de cámaras de seguridad y drones para monitorear el orden de entradas y salidas, la atención y seguridad en caso de emergencias para los civiles y atletas en casos urgentes, identificación facial de presuntos responsables en alteraciones y ataques en los eventos.

equipos internacionales e incluyendo jefes de estado y extranjeros que asistieron y se demostró la importancia de la colaboración para la conclusión segura y exitosa de grandes eventos internacionales.[48]

La planeación de eventos masivos en seguridad es indispensable para crear planes estratégicos en temas de seguridad durante los días del evento, el cómo se transportarán los atletas, la identificación de las personas que entrarán al evento dentro de bases de datos, la seguridad en los alrededores y dentro de las instalaciones que serán sede de estos eventos deportivos para un mayor control en beneficio de atletas, representantes, personal de diversas naciones y civiles.

Como puede apreciarse en este apartado, la utilidad de la inteligencia geoespacial, es diversa, conocida y muy probada.

Ahora la reflexión quedaría bajo el supuesto de, más allá de la Seguridad Nacional y el uso invasivo del de las fuerzas armadas, ya es hora de que la inteligencia geoespacial sea de uso cotidiano en las estrategias de política criminal.

Bauman[49], refería en su obra a un estado que ya vigila todo, todo el tiempo, asemeja el panóptico de antaño, la vigilancia moderna, apunta a observar todo, todo el tiempo para poder resolver problemas pese a sus paradojas respecto del poder invasivo del Estado.

VI. CONCLUSIONES

El México de hoy es producto de más de 30 años de corrupción y desmantelamiento de las instituciones de seguridad. La crisis del sistema mexicano en el paso del estado social y democrático de derecho al estado Liberal, trajo consigo una fragmentación inédita del delito donde se combinó la delincuencia convencional con la delincuencia organizada, permeando las más altas esfera del gobierno

---

48 *Cfr.* NGA. *FIFA World Cup 2010*. National Geospatial-Intelligence Agency. 2016. Véase en: https://www.nga.mil/ABOUT/HISTORY/NGAINHISTORY/Pages/2010FIFAWorldCup.aspx fecha de consulta: enero 2020

49 *Cfr. Bauman, Zygmunt y Lyon David.* Vigilancia Líquida, Barcelona, Paidós, 2017.

qué bajo una tradición corrupta y autoritaria facilitó la descomposición del Estado Mexicano.

La ciudadanía se vió y se ve presa del delito y la violencia como una forma del quehacer cotidiano.

Sin embargo, el uso de la inteligencia geoespacial, conocida y usada para fines militares hoy se presenta como una alternativa para que el nuevo gobierno, cambié la estrategia de control delito, teniendo en tiempo real movimiento de personas, objetos, información de espacios geográficos y procesamiento de información. Dicha tecnología debe de ser apropiada y usada por antes de que la comercialización de la seguridad pudiese ser un arma para los delincuentes. Como ya se dijo algunas instituciones ya usan esta tecnología con fines de investigación o con cierto grado de comercialización por eso es hora de que el Estado tecnifique el control penal.

El Estado Mexicano monopoliza al controlar los satélites y bajo la función de la seguridad pública exclusiva del Estado en mucho podría crear estrategias preventivas exitosas.

El uso de la inteligencia en la información y la tecnología geoespacial debe de ser un hito para evitar la corrupción ya que los procesos de creación y control de la información pueden estar controlados con procedimientos muy rigurosos que identifiquen quién y cómo se usa la información.

Es momento que a partir de dichos controles la información para combatir el delito o para uso preventivo pueda tener una relevancia probatoria en las investigaciones.

Existen ya, marcos legales amplios a nivel internacional y nacional, requerirán ajustes pero será una avanza si se piensa en la política criminal tecnificada.

Tal vez así, con rigurosidad México se aleje de ser califica un narco estado o un estado en descomposición.

VII. FUENTES DE CONSULTA

Bibliografía

Del Palacio Díaz, Alejandro. Agonía y muerte de la Revolución Mexicana, México, UAM-AZC Esquemas.1991.

Del Palacio Díaz, Del Estado de Derecho al Derecho del Estado, México, Leega Omnibus, 1988

Zárate, Alfonso. Un gobierno fallido. Peña Nieto y la sucesión presidencial de 2018, México, Temas de hoy. 2018.

Bauman, Zygmunt, y Lyon David. Vigilancia Líquida, Barcelona, Paidós, 2017.

Hemerografía

Hinostroza, Fernando. "TLC en contexto de la globalización". Revista "A", México UAM-AZC, 1992.

Higuera, J. "Vehículos Aéreos No-tripulados: El escenario latinoamericano". México, Tecnología Militar, Volumen III. 2013. P 2

Fuentes Electrónicas

Bernaldo de Quirós, J. "La Política Geoespacial en el Ministerio de Defensa". España, Instituto Español de Estudios Estratégicos, 2011, p.3. Consultado: 22 octubre del 2018.

Byrne, E.. "Making Drones to Kill Civilians: Is it Ethical?". Springer Science+Business Media, Dordrecht.America. 2015,p.7. . Véase en: https://scholarworks.iupui.edu/bitstream/handle/1805/9741/Byrne_2015_making.pdf?sequence=1, Consultado 18 septiembre del 2018

Hassemer Winfried-Muñoz Conde, Francisco. Introducción a la Criminología y a la Política Criminal. Tirant Lo Blanch. España, Valencia, 2012. Consultado 22 septiembre del 2018.

Lowenthal, Mark M. "Intelligence: From Secrets to Policy". Estados Unidos. Editorial. CQ PRESS & SAGE, chap. 13, 2015, p.413. Amazon (Kindle). Consultado: 10 noviembre del 2018

Olaya, V. "Sistemas de Información Geográfica". España: *CreateSpace Independent Publishing Platform* (Amazon), p7-8, 2014. Consultado: 28 septiembre del 2018.

Rodrigo Hidalgo, M.L. "Las tecnologías de información geográfica y su aplicación al análisis urbano. El caso del estudio de los espacios residenciales cerrados en las áreas metropolitanas de Santiago y Valparaíso". Revista Electrónica de Geografía y Ciencias Sociales. *Universitat* de Barcelona. España, 2004. Véase en: http://www.ub.edu/geocrit/sn/sn-170-31.htm

México el segundo país más violento del mundo. https://www.dw.com/es/estudio-m%C3%A9xico-es-el-segundo-pa%C3%ADs-m%C3%A1s-violento-del-mundo/a-38770281. Consultado: enero 5, 2021.

"Califica AMLO como "narco gobierno" y "gobierno mafioso" a sus antecesores"", *Aristegui Noticias*. https://aristeguinoticias.com/1610/mexico/califica-amlo-como-narcogobierno-y-gobierno-mafioso-a-sus-antecesores/ Consultado: 5 enero del 2020.

Department of the Army. "Geospatial Intelligence Handbook". Washington D.C. United States of America: Department of the Army, p.11, 2011. Consultado: 7 agosto del 2020.

Kovařík, V. "Understanding the Role of Geographic Data and Processes in Geospatial Intelligence". Conferencia Científica y Técnica Internacional, Bratislava, publicación elaborada para la Universidad de Defensa, p.1-7, 2012. Consultado: 14 abril del 2020

United States Navy. Geospatial Intelligence in Joint Operations. Joint Publication, 2(03), 2007,p.15-17, 2017. Consultado: 23 abril del 2020,

Documentos

Los Convenios de Ginebra de 1949 y sus Protocolos adicionales.

Comité Internacional de la Cruz Roja. Ginebra, Suiza. 2010. Consultado 14 octubre del 2018.

United Nations Office for Outer Space Affairs. "Roles and Responsibilities. About us. United Nations". Viena, Austria 2015. Véase en: http://www.unoosa.org/oosa/en/aboutus/roles-responsibilities.html Consultado: Agosto 2020.

Secretaría de Comunicaciones y Transportes. Política Satelital de México. México, Gabinete Legal del presidente de México. 2017, Véase en: http://sct.gob.mx/fileadmin/Direcciones-Grales/Comunicaciones/2017-consulta-publica-politica-satelital.pdf

NGA. FIFA *World Cup* 2010. *National Geospatial-Intelligence Agency.* 2016 en:https://www.nga.mil/ABOUT/HISTORY/NGAINHISTORY/Pages/2010FIFAWorldCup.aspx

Legisgrafía

Ley General para la Prevención Social de la Violencia y la Delincuencia. Cámara de Diputados del Honorable Congreso de la Unión México: DOF, 2012. Véase en http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPSVD.pdf

Ley Federal de Telecomunicaciones y Radiodifusión. México, Cámara de Diputados del Honorable Congreso de la Unión. México: DOF. 2014, Véase en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_150618.pdf

Ley de Seguridad Nacional. México, Cámara de Diputados del Honorable Congreso de la Unión México: DOF. 2015. Véase en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf

SISTEMA FINANCIERO MEXICANO. RETOS DE SEGURIDAD HACÍA LA TRANSFORMACIÓN DIGITAL

José Alejandro González Reyna*
Stephanie Cervantes Razo **

SUMARIO: I. Introducción, II. La seguridad en el ámbito constitucional, III. Esbozo de la importancia del sistema financiero en México, IV. Las transacciones digitales en el sistema financiero mexicano, V. Política criminal en los delitos cibernéticos, VI. Delitos cibernéticos en el sistema financiero, VII. El *phishing*, VIII. El *pharming*, IX. Conclusiones, X. Fuentes de consulta.

I. INTRODUCCIÓN

Hace algunas décadas la forma en que las personas interactúan en sociedad ha sufrido una transformación vigorizante, impactante y en algunos casos atemorizante. Las historias de vida se han ido tejiendo en torno a nuevos modelos de comunicación, comercialización e interacción humana basados en las Tecnologías de la Información y Comunicación (TIC), abriendo el camino a lo que se conoce como la era digital.

Incluso el entendimiento entre las personas ha evolucionado con la transformación digital, construcciones del lenguaje que hoy tienen un sentido y generan una referencia clara, por ejemplo, en una comunicación se puede descubrir con facilidad la referencia de lo

* Maestro en Derecho por la Universidad Nacional Autónoma de México, Facultad de Estudios Superiores Acatlán; actualmente está realizando estudios de Doctorado en Derecho y la Especilidad Derecho Energético, ambas por la Universidad Nacional Autónoma de México, Facultad de Estudios Superiores Acatlán; Profesor de la Licenciatura en Derecho de la Facultad de Estudios Superiores Acatlán y el Posgrado en Derecho de la Facultad de Estudios Superiores Acatlán.

** Estudiante en la especialidad de Derecho Energético por la Universidad Nacional Autónoma de México, Facultad de Estudios Superiores Acatlán; Maestra en Derecho por la Universidad Nacional Autónoma de México, Facultad de Estudios Superiores Acatlán; Profesora de la Licenciatura en Derecho de la FES Acatlán.

que implica *dejar en visto,* o bien, mandar un *whats,* o incluso cuestiones más técnicas como realizar un *SPEI o* bien lo que en el sistema financiero implica el *Fintech.*

Estas nuevas implicaciones de la cotidianeidad han motivado este artículo, puesto que la interacción social está rodeada de ejemplos que involucran una nueva visión de la forma en la que se relacionan las personas, particularmente en el ámbito económico y de satisfacción de necesidades, se puede pensar en algo muy sencillo como lo es el *comprar un café*, que ha dejado de ser el tradicional sistema de intercambio de *dinero en efectivo* por un producto o servicio, pues el uso de tecnologías digitales ha construido una nueva dinámica para esa interacción como el pago por medios electrónicos, no sólo con una tarjeta bancaria, sino con las llamadas *wallets o monederos electrónicos,* incluso, con el uso de plataformas digitales con código QR.

Este artículo tiene como objetivo evidenciar los retos de seguridad y las políticas gubernamentales encaminadas a brindar certeza y seguridad, no sólo al nuevo modelo del sistema financiero, sino a la población que hoy más que nunca está *obligada* de uno u otro modo a interactuar en el sistema digital para la satisfacción de sus necesidades cotidianas.

II. LA SEGURIDAD EN EL ÁMBITO CONSTITUCIONAL

Antes de abordar el tema central de este artículo acerca de los retos que representa la seguridad en el contexto digital, se estima preciso considerar algunos aspectos normativos de rango constitucional, en particular los deberes constitucionales que se estiman relevantes para ubicar la labor del Estado Mexicano en salvaguardar este derecho.

El punto de partida se encuentra en el contenido del artículo 1° de la Constitución Política de los Estados Unidos Mexicanos (CPEUM). En este precepto se han establecido las bases de reconocimiento de los derechos fundamentales de las personas que estén

dentro del territorio nacional, fijando las bases de un sistema de protección de esos derechos.

Retomando las ideas de Ferdinand Lasalle, en un sistema jurídico el reconocimiento e incorporación de los derechos fundamentales son producto de la necesidad, lo que implica que estos derechos sean el sustento del sistema jurídico en sí.

> Pero las cosas que tiene un fundamento no son como son por antojo, pudiendo ser también de otra manera, sino que son así porque necesariamente tiene que ser. El fundamento a que responden no les permite ser de otro modo. Sólo las cosas carentes de un fundamento, que son las cosas casuales y fortuitas, pueden ser como son o de otro modo cualquiera. Lo que tiene un fundamento no, pues aquí obra la ley de la necesidad.[1]

De lo anterior se puede decir, que en el contenido constitucional, los derechos y las garantías de los mismos, que se han incorporado en la norma fundamental, son resultado de los factores reales de poder o de las relaciones que resultan irreductibles para el funcionamiento armónico de la sociedad y el adecuado ejercicio del poder político, en diversos ámbitos de interacción, como lo puede ser el ámbito de la vida, la libertad, la dignidad, la democracia, el patrimonio, el económico, la seguridad, por mencionar algunos.

En el caso de México, la CPEUM como ley fundamental ha precisado mecanismos necesarios para la protección de estos derechos reconocidos como fundamentales, incorporando como mandato esencial para el Estado obligaciones específicas que los vincula a una serie de acciones u omisiones que deberán ser atendidas por las autoridades que ejecuten la función estatal; las que de acuerdo al contenido del mismo precepto constitucional implica la obligación de que los derechos humanos sean *garantizados, promovidos, protegidos y respetados,* ya sea que estén reconocidos en la CPEUM, en los trata-

1 Lassalle Ferdinand. ¿Qué es una constitución?, Vigésima Edición, Coyoacán Editores, traducción de W. Roces Suárez, impreso en México, 2017, pág. 44.

dos internacionales vinculantes para México, o bien en las normas emanadas del Congreso de la Unión que se consideren como ley suprema.

Bajo la premisa anterior, el primer cuestionamiento que surge es determinar cuáles son los límites o cómo debe entenderse cada una de estas obligaciones del Estado a fin de que, por un lado, el Estado cumpla con ellas, y por otro, las personas puedan determinar si las conductas de los órganos del Estado, son acordes al mandato constitucional en materia de los derechos fundamentales.

Ante esta necesidad, las máximas autoridades jurisdiccionales de México, han emitido criterios con rango de jurisprudencia, a través de los cuales busca definir en qué consisten tales obligaciones del Estado. Por cuanto hace a la obligación de *garantizar* los derechos humanos, en el criterio correspondiente a la décima época, identificado con el número de registro 2008515, publicado en la Gaceta del Semanario Judicial de la Federación, en el libro 15, del mes de febrero de 2015, con número de identificación de tesis XXVI-I.3o. J/24 (10a.), denominada DERECHOS HUMANOS. OBLIGACIÓN DE GARANTIZARLOS EN TÉRMINOS DEL ARTÍCULO 1o., PÁRRAFO TERCERO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS[2], los máximos tribunales del país han precisado los alcances e implicaciones de dicha obligación, por lo que analizando dicho criterio se puede precisar que la obligación de *garantía* de los derechos fundamentales implica para el Estado lo siguiente:

1. En primer lugar, *la finalidad de esta obligación es la realización del derecho fundamental*, es decir, que se puedan materializar los derechos humanos en las actividades diarias de la población.
2. *La eliminación de restricciones al ejercicio de los derechos*, es decir, que los actos de las autoridades en todo caso deberán evitar convertirse en un obstáculo para el ejercicio de los derechos humanos de la población.

2 Jurisprudencia consultada el día 22 de junio de 2020 en la página *https://sjf.scjn.gob.mx/sjfsist/paginas/tesis.aspx*

3. *La provisión de recursos o la facilitación de actividades que tiendan a lograr que todos se encuentren en aptitud de ejercer sus derechos fundamentales*. Este punto, entre otras cosas, implica el que se cuente con los instrumentos normativos e institucionales para el ejercicio del derecho fundamental de que se trate o bien su defensa.

Según lo explica el criterio judicial, las acciones que en su caso ejecute el Estado como parte de su deber de garantizar el ejercicio de los derechos humanos, requiere que el Estado, a través del órgano específico vinculado al ejercicio del derecho humano del que se trate, *tenga conocimiento de las necesidades de las personas o grupos involucrados*, es decir, que en el caso de la seguridad en el sistema financiero mexicano, los órganos encargados de garantizar la misma, tienen el deber de investigar, sancionar y reparar las violaciones o afectaciones de los derechos patrimoniales de las personas que formen parte de dicho grupo, ya sean los usuarios del servicio financiero o bien los propios prestadores de servicios financieros.

Este obligación de garantía, desde luego tiene una relación ineludible con la obligación de protección de los derechos fundamentales a cargo del Estado, respecto de la cual los tribunales judiciales, del mismo modo, han tratado de definir y explicar en qué consiste tal obligación, a fin de tener parámetros para determinar su debido cumplimiento, así en el criterio correspondiente a la décima época, identificado con el número de registro 2008516, publicado en la Gaceta del Semanario Judicial de la Federación, en el libro 15, del mes de febrero de 2015, con número de identificación de tesis XXVII.3o. J/25 (10a.), denominada DERECHOS HUMANOS. OBLIGACIÓN DE PROTEGERLOS EN TÉRMINOS DEL ARTÍCULO 1o., PÁRRAFO TERCERO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS[3], se han establecido los alcances de la obligación en comento, destacándose de dicho criterio la expresión de la autoridad jurisdiccional, res-

3 Jurisprudencia consultada el día 22 de junio de 2020 en la página *https://sjf.scjn.gob.mx/sjfsist/paginas/tesis.aspx*

pecto de las consideraciones básicas del deber de protección de los derechos humanos por parte del Estado, haciendo consistir dicha obligación en dos elementos:

1. Prevenir violaciones a los derechos fundamentales, ya sea que provengan de una autoridad o de algún particular.
2. Contar con mecanismos de vigilancia como de reacción ante el riesgo de vulneración del derecho, a fin de impedir la consumación de la violación.

Lo sostenido por los máximos tribunales jurisdiccionales del país, hace referencia a un operador deóntico de *hacer* como obligación del Estado, puesto que, por virtud de la misma, la autoridad debe desplegar conductas a fin de evitar que el ejercicio de un derecho fundamental sea vulnerado.

Otra obligación que cobra relevancia para los efectos de este artículo, lo es la obligación de *promoción* de los derechos fundamentales a cargo del Estado, la cual del mismo modo que las anteriores ha sido definida y delimitada por la autoridad judicial, mediante el criterio correspondiente a la décima época, identificado con el número de registro 2007597, publicado en la Gaceta del Semanario Judicial de la Federación, en el libro 11, del mes de octubre de 2014, con número de identificación de tesis XXVII.3o. 4 CS (10a.), denominada DERECHOS HUMANOS. OBLIGACIÓN DE PROMOVERLOS EN TÉRMINOS DEL ARTÍCULO 1o., PÁRRAFO TERCERO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, criterio del cual se destaca que la finalidad de dicha obligación atribuye al Estado los deberes siguientes:

1. Conocimiento. En la medida que implica que el Estado debe facilitar a los gobernados el que tengan claridad y conocimiento de sus derechos, y las formas que tienen para defenderlos.
2. Ampliación. Este punto se puede interpretar precisamente como un deber de la actividad del Estado de lograr el alcance de las personas

que puedan conocer sus derechos y mecanismos de protección, para lograr su realización.

3. Informar. Esto implica la labor del Estado tendiente a mantener una campaña permanente de divulgación de los derechos y mecanismos para su ejercicio, a fin de que las personas puedan disfrutar sin restricción alguna sus derechos.

Ahora bien, dentro de la construcción constitucional de deberes y obligaciones a cargo del Estado, así como de los derechos de las personas, con relación a la seguridad de la información, se puede destacar el contenido de algunos preceptos constitucionales asociados a la *seguridad de las personas en el ámbito digital*. El primero de ellos sería el artículo 6° constitucional, que en años recientes ha incorporado en el sistema constitucional el derecho a la información conocido como *habeas data* y por otro lado una garantía o herramienta para la protección de los datos de las personas en cuatro dimensiones que son acceso, rectificación, cancelación y oposición del tratamiento de sus datos personales, ya sea que este en posesión del Estado o de particulares (derechos ARCO), lo que se ha incorporado de igual forma en el segundo párrafo del artículo 16 de la CPEUM.

En general se podría decir que del precepto constitucional se desprenden cuatro principales derechos: el derecho a la intimidad, el derecho a la privacidad, el derecho a la autodeterminación informativa y el derecho a la confidencialidad.

> La intimidad es el derecho a no ser conocidos, en ciertos aspectos, por los demás. Es un derecho al secreto, a que los demás no sepan lo que somos o lo que hacemos[4]

Se trata así del derecho que tenemos al anonimato de ciertas conductas o aspectos de nuestra persona o nuestra vida. Acompañado de este derecho, se encuentra el derecho a la privacidad, que es un derecho que va asociado al control que es posible tener respecto de la restricción o acceso a información propia "el derecho a la privaci-

4 Villanueva, Ernesto y Diaz Vanessa. *Derecho de las nuevas tecnologías. En el siglo XX derecho informático"*, Editorial Oxford, México, año 2015, pág. 22.

dad no representa sino la expectativa individual de control que cada persona tiene respecto de la información sobre sí mismo y la forma en que esta información es conocida o utilizada por terceros".[5]

En el entendimiento de los dos derechos anteriores, el de la *intimidad y privacidad,* surge el derecho a la *autodeterminación informativa* de la información, que es entendida como la atribución en la que "el titular de la información o dato debe mantener control de lo que sobre su persona se ha recabado y se mantiene en archivos o en los bancos de datos informatizados, dando paso con ello al reconocimiento del derecho que se tiene de acceso y control de dicha información."[6]

Finalmente, el derecho a la confidencialidad "se resguarda en la confianza depositada en otro, quien se vale de su propia conducta para mantener el ocultamiento"[7]. Así en términos generales, la configuración constitucional ha establecido lineamientos específicos para reconocer el derecho de las personas al tratamiento de sus datos y por otro lado, los mecanismos de defensa de su información colocada en manos de terceros.

Un aspecto importante a considerar en relación con todos estos derechos y sus garantías, lo es el uso de las *tecnologías de la información y comunicación* (TIC) como una herramienta fundamental en el ejercicio del derecho de acceso y protección de la información, así como en los mecanismos de prevención a cargo del Estado Mexicano, tal y como se aprecia del contenido del párrafo tercero del artículo 6° de la CPEUM, que le ha incorporado como un derecho fundamental, tal y como se abordará más adelante.

Finalmente, la protección de los derechos y pertenencias de las personas implica labores específicas de seguridad, que de forma originaria el texto constitucional a confiado al Estado como una labor sustancial de ser. En este contexto, el artículo 21 de la CPEUM precisa en el párrafo noveno que:

---

5 *Ibídem, pág. 25.*

6 *Ibídem, pág. 26.*

7 *Ibídem, pág. 28.*

> La seguridad pública es una función del Estado a cargo de la Federación, las entidades federativas y los Municipios, cuyos fines son salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como contribuir a la generación y preservación del orden público y la paz social, de conformidad con lo previsto en esta Constitución y las leyes en la materia. La seguridad pública comprende la prevención, investigación y persecución de los delitos, así como la sanción de las infracciones administrativas, en los términos de la ley, en las respectivas competencias que esta Constitución señala. La actuación de las instituciones de seguridad pública se regirá por los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos reconocidos en esta Constitución.[8]

Con todo lo anterior, se puede tener una visión concreta de las implicaciones constitucionales de seguridad de la información, así como las obligaciones normativas para el Estado en el ámbito de la protección y salvaguarda de los derechos patrimoniales y personales de las personas, ateniendo a una doble obligación, por un lado el impulso de las TIC en los diversos sectores de la sociedad, como un derecho fundamental, y por otro lado, el tener mecanismos que garanticen la seguridad en el ejercicio de este derecho en plataformas digitales.

III. ESBOZO DE LA IMPORTANCIA DEL SISTEMA FINANCIERO EN MÉXICO

No hay duda de que cualquier aspiración de políticas públicas (económicas) del gobierno que se trate, busca, aún sea en el discurso, el crecimiento y el desarrollo económico. El primer concepto, se refiere a "un fenómeno objetivo, por lo que puede observarse y medirse. Significa el aumento de las actividades económicas de un

8 Artículo 21 de la Constitución Política de los Estados Unidos Mexicanos, consultado el día 23 de junio de 2020, en *http://www.diputados.gob.mx/LeyesBiblio/pdf/1_080520.pdf.*

país y en él se manifiesta la expansión de las fuerzas productivas"[9]. Por otro lado, el desarrollo "es el proceso mediante el cual los países pasan de un estado atrasado en su economía a un estado avanzado. Este grado alcanzado en el desarrollo representa mejores niveles de vida para la población en su conjunto, supone que los niveles de vida mejoran día con día, lo que representa cambios cuantitativos y cualitativos."[10]

En este sentido, las políticas económicas asumen un papel importante en las aspiraciones de cualquier gobierno que pretenda el mejoramiento de las condiciones de vida de sus habitantes, a fin de lograr el crecimiento y desarrollo económico al que se aspira tanto en lo individual como en lo colectivo.

Ahora bien, dentro estas políticas económicas encontramos de forma particular la *política financiera* que es la que "se encarga de formular objetivos, señalando los instrumentos adecuados para controlar los ingresos y administrarlos, así como para elaborar el gasto del sector público. La política financiera se encarga también del sistema bancario, así como la política monetaria y crediticia."[11] Por lo anterior, es dable considerar que, como parte de las estrategias que se plantea cualquier gobierno, de forma ineludible está el de la política económica que permita por un lado el crecimiento económico y por el otro el desarrollo económico.

Ahora bien, para lograr estos objetivos, el gobierno debe permitir la interacción en el sistema financiero de las instituciones crediticias, que tienen un papel fundamental en el flujo de capital del país, aunado al hecho de que tiene el contacto directo y de primera mano con la población por cuanto hace a la interacción de intercambio de dinero, la satisfacción de las necesidades cotidianas, incluyendo las del ahorro, resguardo de dinero, financiamiento, inversión, por mencionar algunas.

---

9 Mendez Morales, José Silvestre. *Problemas económicos de México y sustentabilidad*. Séptima edición, 2012, Mc Graw Gill, México, pág. 42.

10 *Ídem.*

11 *bídem*, pág. 199.

El sistema financiero mexicano, por cuanto hace a las instituciones crediticias, han sido englobadas en dos rubros fundamentales, instituciones de banca múltiple (privadas) e instituciones de banca de desarrollo (pública), siendo para efectos prácticos, una clasificación aceptable para los fines de este artículo. En este contexto, se puede afirmar que las instituciones de crédito forman parte de la cadena aspiracional para lograr los objetivos de cualquier política económica, puesto que son estas instituciones las que mantienen la interacción constante entre el capital y las satisfacciones de necesidades cotidianas para el impulso de las actividades productivas y económicas.

Por ejemplo, si una empresa inmobiliaria desea llevar a cabo un complejo habitacional, podría acudir a una institución crediticia o financiera que le brinde el apoyo económico necesario para hacer caminar el proyecto, si una persona desea adquirir un vehículo o una casa, probablemente haga uso de una sistema de crédito hipotecario o automotriz para lograr la satisfacción de esa necesidad, en fin, son muchos ejemplos los que se pueden plantear sobre la importancia de las instituciones crediticias, como parte del sistema financiero mexicano y de las políticas económicas del Estado Mexicano.

Sin embargo, no se trata sólo del hecho de que las instituciones crediticias cuenten con recursos económicos propios que les permita invertir en la satisfacción de las aspiraciones de crecimiento y desarrollo de un país, sino que se trata de un sistema complejo que implica el uso de recurso de otros, es decir, el movimiento del *dinero* que por un lado depositan los usuarios de las instituciones de crédito y por otra el *colocar* dicho dinero en actividades productivas concretas. De acuerdo al autor Humberto Ruiz Torres:

> las instituciones de crédito son de vital importancia para el desarrollo económico de una sociedad, ya que fungen como grandes receptoras y canalizadoras de recursos. Por una parte, reciben créditos del público ahorrador y, por otra, colocan esos recursos mediante el otorgamiento de créditos a las personas físicas, a las empresas o al

> gobierno. Esto lleva a plantear una idea esencial: los bancos operan fundamentalmente con dinero de terceros (el público ahorrador) y no con el propio; de ahí que sea necesario regular con la mayor precisión posible el funcionamiento de los bancos.[12]

Con lo anterior, se puede evidenciar la importancia del *sistema financiero en México,* puesto que se trata de un mecanismo de suma importancia que permite, por un lado, la captación de dinero, y por otro, la inyección de dinero para la satisfacción de necesidades concretas que de forma directa o indirecta impulsan y dan dinamismo a la producción de bienes y servicios, a su vez, la posibilidad de desarrollo de áreas productivas, de allí que el sistema financiero de México, involucre diversas instituciones para su funcionamiento y protección, como lo es la Secretaría de Hacienda y Crédito Público, la Secretaría de Economía, la Comisión para la Defensa de los Usuarios de Servicios Financieros, la Comisión Nacional Bancaria y de Valores, Banco de México, Instituciones de Banca Múltiple y de Banca de Desarrollo.

Instituciones que, en su conjunto, son parte de los mecanismos gubernamentales creados con el fin de mantener, un sistema financiero sano, una competencia económica equilibrada, protección a los gobernados que utilizan el sistema financiero y, sobre todo, brindar una seguridad a todas las partes que participan en el mismo, para impulsar y fomentar un dinamismo en el sector, que impulse y de condiciones para alcanzar esas aspiraciones de desarrollo económico.

IV. LAS TRANSACCIONES DIGITALES EN EL SISTEMA FINANCIERO MEXICANO

Cada día existe un cúmulo de expectativas que van alimentando las aspiraciones de las personas, quizá algunas de estas expectativas están en aprovechar de *mejor manera el tiempo* para ejecutar actividades cotidianas; desde pagar la tarjeta de crédito, comprar algún artícu-

12 Ruiz Torres, Humberto. E*lementos de derecho bancario*. Editorial Mc Graw Hill, México, pág. 1.

lo, llegar más rápido algún lugar, comunicarse con alguien, enviar algún documento, hacer la tarea, o simplemente ver el programa favorito de televisión o escuchar esa canción que inspira o motiva el concluir ese día.

Se trata de una aspiración diaria de encontrar la forma de lograr la mayor eficiencia en las actividades que permita no sólo satisfacer una necesidad concreta, sino además lograr el menor esfuerzo o costo al respecto. Las tecnologías han encontrado un lugar privilegiado entre las estrategias para lograr la eficiencia operativa e incluso económica en la satisfacción de las necesidades cotidianas, y en el sistema financiero de México no es la excepción.

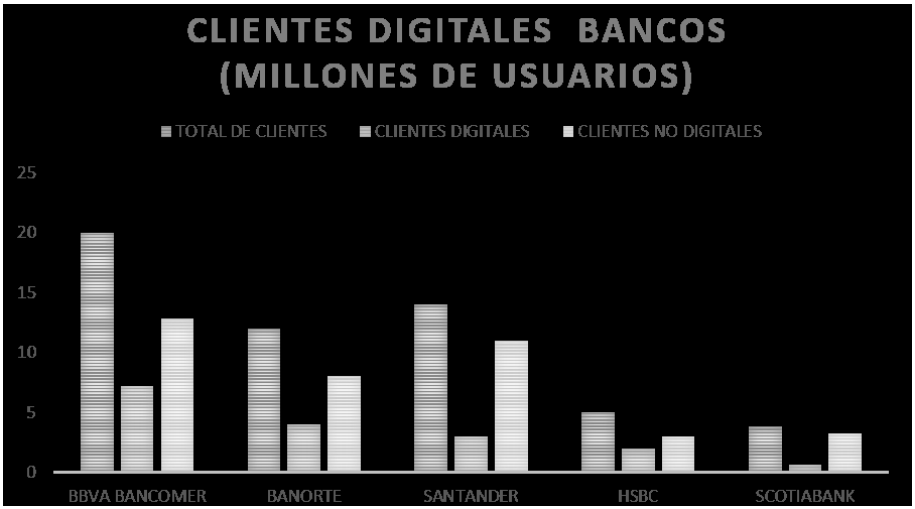
Hoy en día, muchas instituciones de crédito han buscado emplear las tecnologías para hacer más eficiente su operación, normalmente con un énfasis económico más que técnico, lo que poco a poco se ha posicionado como una parte toral de sus actividades, impulsando el uso de tecnologías para el funcionamiento de las operaciones financieras, que haga más fácil la captación y disposición de recursos económicos para los usuarios de servicios financieros.

En el mes de septiembre de 2019, el periódico el Economista, publicó un artículo de Edgar Suárez, en el que se refleja el dinamismo de las instituciones bancarias y su migración hacia las tecnologías digitales para lograr la satisfacción de las necesidades de su clientela, así como sus propias necesidades de hacer eficiente su operación.

De la investigación hecha por el periodista, destaca la identificación de instituciones de crédito que han hecho procesos de captación y colocación de recursos a través de mecanismos digitales.[13] Estos datos se muestran en la siguiente gráfica que permitirán vislumbrar el impacto de los mecanismos digitales en la operación bancaria.

---

13 Banca Mexicana acelera hacia lo digital. Nota del día 20 de marzo de 2019. Fecha de consulta 01 de septiembre de 2019. *https://www.eleconomista.com.mx/sectorfinanciero/Banca-mexicana-acelera-hacia-lo-digital-20190320-0036.html*



De los datos aportados en la nota periodística tenemos que tan solo de estas instituciones bancarias existen 54.8 millones de usuarios de servicios financieros, de los cuales 16.8 millones utilizan servicios de banca digital, es decir, que casi el 30% (treinta por ciento) de usuarios bancarios hacen uso de estas nuevas tecnologías para satisfacer alguna necesidad concreta de disposiciones o colocación de sus recursos económicos.

Ahora bien, de acuerdo a esta nota, el gobierno federal actual tiene como objetivo es la *bancarización* de la población a fin de incorporarlos al sistema financiero formal. Sea cual fuere la estrategia que el gobierno tenga para lograr este fin, es evidente que la tendencia en el sistema financiero mexicano lo es el impulso de las estrategias de medios digitales para la operación del servicio financiero.

Esta tendencia incluso ha dado pauta a una nueva manera de realizar operaciones bancarias, como lo es el *Fintech.* De acuerdo a la Comisión Nacional para la Protección y Defensa de Usuarios de Servicios Financieros (CONDUSEF), el *Fintech* se puede entender de la siguiente manera:

> El término "Fintech" deriva de las palabras "finance technology" y se utiliza para denominar a las empresas que ofrecen productos y servicios financieros, haciendo uso de tecnologías de la información y comunicación, como páginas de internet, redes sociales y aplicaciones para celulares. De esta manera prometen que sus servicios sean menos costosos y más eficientes que los que ofrecen la banca tradicional. Actualmente operan alrededor de 158 *Fintech* en el país.[14]

Se trata pues de *instituciones crediticias* que operan con recursos de terceros, es decir, captan dinero de inversionistas y lo colocan en instrumentos de deuda, de tal modo que hacen una intermediación directa o indirecta entre la persona que desea invertir y aquellas personas que requieren instrumentos de financiamiento; quizá una de las cosas que más llama la atención de la información proporcionada por la CONDUSEF sea precisamente la falta de regulación de todo el universo de operaciones que se realizan a través de medio digitales en materia financiera.

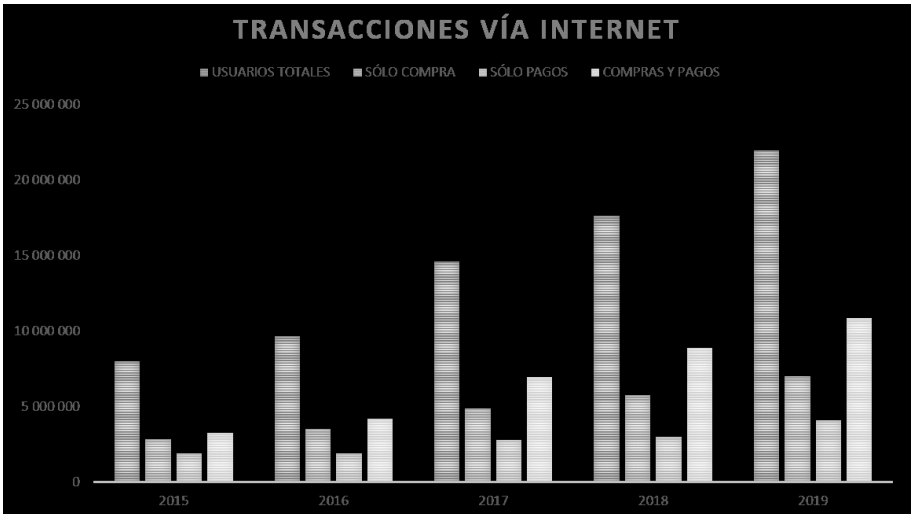
En este contexto, para el desarrollo de las actividades financieras a través de las TIC en el sistema financiero, es necesario la ocupación de personas que desarrollen u operen dichas TIC, para materializar y explotar esta actividad mediante el uso de plataformas digitales. El 10 de junio de 2019, el Instituto Nacional de Estadística y Geografía (INEGI) dio a conocer la *estadística a propósito de las ocupaciones relacionadas con las tecnologías de la información y de la comunicación datos nacionales*.

De dicha estadística destaca que al cuarto trimestre de 2018 alrededor de 752 mil personas tienen como ocupación alguna actividad relacionada a las TIC. En la misma estadística destaca que las ocupaciones más demandadas en el mercado laboral de las TIC son las relacionadas con desarrolladores de sistemas de cómputo, expertos en ciberseguridad, científicos de datos, analistas de *malwer* y *hacker*

---

14 Educación Financiera. CONDUSEF, fecha de consulta 01 de septiembre de 2019. *https://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/educacion-financiera/763-que-son-las-fintech*

ético, entre otras.[15] En la siguiente gráfica, se puede apreciar de mejor forma la actividad ocupacional en las TIC, de acuerdo a la encuesta elaborada por el INEGI:



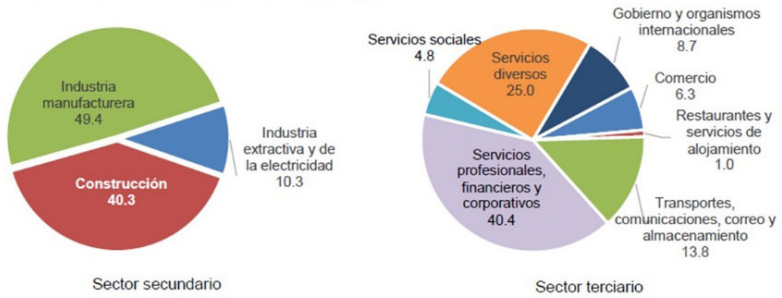
De los datos anteriores, destaca que el sector financiero, corporativo y de servicios profesionales, es en el que se han ocupado mayores profesionales de las TIC, lo que permite encontrar una cierta coincidencia con lo expresado en la nota periodística antes comentada, puesto que, en el caso del sector financiero mexicano, se ha buscado impulsar servicios a través de plataformas y tecnologías digitales para la materialización de servicios financieros.

En este contexto, el INEGI ha realizado un análisis de datos relacionados con el uso de TIC en diferentes actividades cotidianas, destacando información acerca de las transacciones que se han realizado mediante el uso de TIC, en este caso, transacciones hechas a través de Internet. Esta información refleja a usuarios que han realizado compras, pagos o ambos, a través de la red, durante el periodo comprendido de 2015 a 2019.

15 Información obtenida de *https://www.inegi.org.mx/*, consultada el 23 de mayo de 2020.

De acuerdo a estos datos, de 2015 a 2019 se ha triplicado el número de personas que usan el Internet para realizar alguna transacción, pasando de 7´992,438 en 2015 a 21´930,357 para 2019. A fin de clarificar lo anterior, se ha elaborado la siguiente gráfica, con los datos obtenidos del INEGI[16]:

Distribución de la población de 15 años y más ocupada en las TIC por principales sectores económicos en que se desempeña, 2018 *Gráfica 5*



Nota: No incluye información insuficientemente especificada.
Fuente: **INEGI**. Encuesta Nacional de Ocupación y Empleo, ENOE. Cuarto trimestre de 2018.

De los datos anteriores, surge la inquietud de analizar las dificultades y problemas de la nueva era de *digitalización* de los servicios financieros, puesto que así como ha abierto un nicho de oportunidad para la creación de nuevos mecanismos e instrumentos para la operación de servicios y transacciones financieras, también se ha creado un nuevo esquema en la operación del *crimen* a través de medios digitales, que ponen en riesgo el capital de los particulares, y deja en una situación de vulnerabilidad a su patrimonio, a través de los llamados delitos digitales.

16 Datos obtenidos de *https://www.inegi.org.mx/temas/ticshogares/default.html#Tabulados*, consultado el 04 de junio de 2020.

V. POLÍTICA CRIMINAL EN LOS DELITOS CIBERNÉTICOS

Como se ha visto anteriormente, en los últimos años se ha incrementado significativamente el uso de recursos y medios digitales para la realización de actividades cotidianas, en especial transacciones a través de la red, incremento que lamentablemente ha presentado nuevos riesgos, nuevas necesidades de acción y mejoras en las herramientas y recursos digitales, para poder abatir errores o fallas técnicas, o bien, *arteros ataques* de personas que tienen el conocimiento y dominio de estos medios y recursos.

El pasado 10 de agosto del año 2019, el periódico *El Financiero*, hizo pública los errores en un *Data Center* (un centro de procesador de datos con arquitectura de informática de red) que ocasionó que muchos usuarios de los recursos digitales no pudieran disponer de su dinero para la satisfacción de sus necesidades de adquisición de productos o servicios.[17] En marzo y abril del año 2018, *hackers* hicieron evidente las deficiencias de los sistemas de seguridad en materia de banca digital, mediante un *ciberataque* que hasta hoy se ha considerado el más importante que sufrió el sistema financiero mexicano; este ataque dio como resultado una pérdida de 300 millones de pesos.[18]

Los anteriores ejemplos reflejan no sólo de la necesidad de que las instituciones bancarias mejoren o incluso implementen mecanismos de seguridad digital, a fin de proteger los recursos económicos de las personas, sino además la necesidad de que el Estado Mexica-

---

17 Leyva Jeanette, "Falla en data center genera caos en el uso de tarjetas en México", periódico *el financiero*. Publicación del 10 de agosto de 2019. Nota consultada 01 de septiembre de 2019. *https://www.elfinanciero.com.mx/economia/falla-en-data-center-genera-caos-en-el-uso-de-tarjetas-en-mexico.*

18 S/A "Hackers detrás de ataques al SPEI, estuvieron dentro de las redes de los bancos por año y medio ", periódico *el Economista*. Publicación 07 abril 2019. Nota consultada el día 01 septiembre de 2019. *https://www.eleconomista.com.mx/sectorfinanciero/Hackers-detras-del-los-ataques-al-SPEI-estuvieron-dentro-de-las-redes-de-los-bancos-por-ano-y-medio-20190407-0018.html*

no mejore e implemente políticas públicas en materia de seguridad y de combate a la criminalidad, en particular, en el rubro de la banca digital.

En este sentido, el impulso de las TIC y desde luego, la creación de mecanismos de protección en el ámbito digital, además de una necesidad, es un compromiso que se ha adoptado a nivel internacional, del que se desprende la preocupación de lograr compaginar las TIC con la satisfacción de las necesidades sociales. Ejemplo de esto es la declaración de principios de la Cumbre Mundial sobre la Sociedad de la Información, organizada por las Naciones Unidas, celebrada en Túnez en el año 2005.

Como resultado de esta cumbre, los estados participantes reconocieron:

> que la educación, el conocimiento, la información y la comunicación son esenciales para el progreso, la iniciativa y el bienestar de los seres humanos. Es más, las tecnologías de la información y las comunicaciones (TIC) tienen inmensas repercusiones en prácticamente todos los aspectos de nuestras vidas. El rápido progreso de estas tecnologías brinda oportunidades sin precedentes para alcanzar niveles más elevados de desarrollo. La capacidad de las TIC para reducir muchos obstáculos tradicionales, especialmente el tiempo y la distancia, posibilitan, por primera vez en la historia, el uso del potencial de estas tecnologías en beneficio de millones de personas en todo el mundo.[19]

De tal reconocimiento se aprecia la importancia que las TIC, como una nueva forma de vivir e interactuar en diversos sectores, incluso siendo un factor importante para alcanzar niveles de desarrollo económico. Aunado a esto, como se ha visto con antelación, el uso de las TIC representa retos de seguridad, que permitan estimular el uso de las mismas, como un mecanismo viable y fiable, en particular

---

19 Cumbre Mundial sobre la Sociedad de la Información, Documento WSIS-03/GENEVA/4, Naciones Unidas, consultado en *https://www.itu.int/net/wsis/docs/geneva/official/dop-es.html*, el día 22 de mayo de 2020.

en el sector financiero; por ello, en esta cumbre se reconoce del mismo modo que la seguridad es una condicionante ineludible para el fomento de las TIC, puesto que sólo así, se podrá lograr el impulso deseado en el uso de la tecnología, en un ambiente confiable:

> El fomento de un clima de confianza, incluso en la seguridad de la información y la seguridad de las redes, la autenticación, la privacidad y la protección de los consumidores, es requisito previo para que se desarrolle la Sociedad de la Información y para promover la confianza entre los usuarios de las TIC. Se debe fomentar, desarrollar y poner en práctica una cultura global de ciberseguridad, en cooperación con todas las partes interesadas y los organismos internacionales especializados. Se deberían respaldar dichos esfuerzos con una mayor cooperación internacional. Dentro de esta cultura global de ciberseguridad, es importante mejorar la seguridad y garantizar la protección de los datos y la privacidad, al mismo tiempo que se amplía el acceso y el comercio. Por otra parte, es necesario tener en cuenta el nivel de desarrollo social y económico de cada país, y respetar los aspectos de la Sociedad de la Información orientados al desarrollo.[20]

Con lo anterior, podemos darnos cuenta de que los organismos internacionales contemplan la mejora y el avance, para proteger a la población de la inseguridad en el uso de las TIC, en la realización de las actividades financieras.

A nivel internacional ha estado latente el tema de la seguridad de la información y la protección del usuario en el Internet, es por ello que los países han tenido que adoptar diversos términos que permiten identificar las acciones que se realizan de manera ilícita con la utilización de las tecnologías de la información y comunicación.

Es por ello, que resulta necesario definir que son los delitos cibernéticos, los cuales han dado origen a la implementación de políticas internas de *ciberseguridad* que han permeado en acciones de índole internacional.

---

20 *Ídem.*

VI. DELITOS CIBERNÉTICOS EN EL SISTEMA FINANCIERO

Para el autor Muñoz Torres el delito cibernético es aquel que "tipifica las acciones realizadas por una persona como ilegal cuando dicho acto tiene la finalidad de afectar las comunicaciones que se llevan a cabo a través de las Tecnologías de la Información y Comunicación"[21]. De acuerdo al autor un elemento primordial para llevar el menoscabo y llevar a cabo este tipo de actividades ilícitas es la utilización de las herramientas tecnológicas.

El 23 de noviembre del año 2001 se llevó a cabo por parte del Consejo de Europa, la Convención sobre Ciberdelincuencia, en Budapest, la cual fue un parteaguas para identificar las acciones que cada país debe adoptar para implementar medidas para combatir el delito cibernético o atacar la *cibercriminalidad.* En esta Convención "se reconoce y asume la posibilidad de aludir conductas delictivas tras las fronteras del país de comisión del delito".[22]

Para los autores Villanueva y Díaz la Convención busca:

> equiparar al *cibercrimen* como un delito convencional; es decir, como una amenaza interna, de la cual los Estados deben desarrollar una política criminal común. Los Estados deben criminalizar la mayor parte de: a) varias actividades que tienen en la mira los sistemas informáticos y los datos; b) la falsificación informática; c) los fraudes informáticos; d) el uso de la tecnología cibernética para crear, distribuir o procesar pornografía infantil, y e) el uso de la tecnología cibernética para cometer infracciones a la propiedad intelectual.[23]

Como nos podremos dar cuenta en esta Convención se establecieron estrategias que cada país debe adoptar para poder contrarrestar esta actividad criminal, de la misma manera clasifica a los delitos de acuerdo a los diversos actos:

---

21 Villanueva Ernesto, Díaz Vanessa, *op. cit.,* pág. 66.

22 *Ibídem*, pág. 67.

23 *Ídem.*

- Delitos contra la confiabilidad, la integridad, y la disponibilidad de los datos y sistemas informáticos.
- Delitos informáticos
- Delitos relacionados con el contenido, y
- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.[24]

En esta clasificación se engloban las diversas acciones con relación a la información y al tratamiento que se le puede dar a esta, propiciando las conductas de violación a la confidencialidad, integridad, disponibilidad de la información, robo de información, robo de identidad, fraude, la utilización ilícita de dispositivos electrónicos, falsificación, etc.

La proliferación de la información a través de la red, ha ocasionado que en esta nueva tendencia de la sociedad global exista la necesidad por parte de cada país de desarrollar una actualización de las conductas que permitan salvaguardar los derechos de los usuarios.

En este mismo sentido, resulta importante hacer mención de la dinámica que trae como consecuencia la realización de estos actos, para ello la autora Laura Mayer Lux define *cyber criminology* como "el estudio de la comisión de crímenes que se llevan a cabo en el ciberespacio y su impacto en el espacio físico"[25]

Dentro de la clasificación de los delitos que existen para poder determinar la conducta del criminal en las actividades financieras, se encuentra el fraude informático, para la autora Laura Mayer el "fraude informático evoca la producción de un perjuicio patrimonial a través de la alteración o manipulación de datos o programas de sistemas informáticos"[26], para la realización de este acto es necesario que el criminal conozca el sistema de una red privada y así poder violarla o puede ser manipulada desde adentro.

---

24 *Ibídem*, pág. 68.

25 Mayer Lux, Laura, *Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos*, Revista Ius et Praxis, Año 24, Nº 1, 2018, *https://scielo.conicyt.cl/pdf/iusetp/v24n1/0718-0012-iusetp-24-01-00159.pdf,* pág. 163, fecha de consulta 28 octubre 2020.

26 *Ibídem*, pág. 173.

Para ello establece la autora que es necesario profundizar en esta conducta ya que suele identificarse con diversos comportamientos, que muchas veces corresponden a etapas de ejecución imperfecta e incluso a actos preparatorios de un fraude propiamente dicho.[27]

VII. EL *PHISHING*

Como hemos visto anteriormente, los delitos cibernéticos se pueden clasificar de acuerdo a su finalidad, para el presente artículo es menester abordar el delito relacionado con las operaciones financieras, el cual es el *phishing*, en este "se obtienen de manera fraudulenta los datos de identidad personal de clientes de bancos y de sus cuentas bancarias o tarjetas de crédito, destinados a efectuar transacciones electrónicas en favor del agente o de terceros. La obtención de tales datos puede lograrse a través de diversos medios, que incluyen desde la denominada ingeniería social, hasta la afectación del soporte lógico de un sistema informático"[28]

En el *phishing* la actividad ilícita va encaminada a la obtención de información de los usuarios cuando realizan diversas actividades (transferencias, comercio, pagos gubernamentales, etc), a través de los sistemas que implementan las diversas instituciones financieras.

El desarrollo de este delito fue evolucionando con ayuda de las TIC y la misma autora establece que dentro de sus "primeras variantes, el *phishing* implicó el envío de correos *spam* masivos e indiscriminados, supuestamente provenientes de fuentes fiables, en los que se les solicitaba a los receptores la entrega de información relativas a sus cuentas, a veces bajo la amenaza de que, en caso de no ser proporcionadas, éstas serían canceladas o bloqueadas".[29]

---

27 *Ibídem*, pág. 174.
28 *Ídem.*
29 *Ídem.*

Esto ocasionó que los bancos adoptaran medidas informativas y preventivas, para combatir los riesgos de los usuarios en los sistemas implementados por las instituciones financieras, procurando dar certeza y seguridad en la utilización de las diversas plataformas.

> Sin embargo, el *phishing* "se extendió a otros comportamientos, como el uso de un *malware*[30] que, para obtener informaciones sensibles, ataca directamente las operaciones que realiza la víctima. Adicionalmente, se hace posible que el *phisher* se limite a obtener fraudulentamente los datos de identidad personales de los clientes del banco y de sus cuentas bancarias o tarjetas de crédito y los comercialice a fin de que sean otros quienes perjudiquen el patrimonio de la víctima. O bien, que operen intermediarios (también conocidos como "mulas"), que facilitan -consciente o inconscientemente- sus cuentas bancarias para recibir el dinero obtenido fraudulentamente, y luego lo traspasan al autor del fraude".[31]

Las herramientas tecnológicas han sido un factor importante en la comisión y transformación de los delitos y uno de los medios idóneos que han encontrado los criminales para llevar a cabo la comisión de este tipo de delitos es la red.

VIII. EL *PHARMING*

Otro delito relacionado a las operaciones financieras es el "*pharming* el cual implica la creación y operación de una página web falsa, muy parecida o igual a la de una entidad, fundamentalmente bancaria o de otra naturaleza, como un sitio de subastas (por ejemplo, *eBay*). En este caso, puede ocurrir que el usuario ingrese el nombre del banco en un buscador (*v. gr., Google*) o la dirección *web* de la entidad bancaria en la barra de direcciones y sea dirigido a una página *web* fraudulenta". [32]

---

30 Son aquellos programas o partes de ellos que tienen un efecto malicioso en la seguridad de tu ordenador. Este término engloba muchas definiciones como "Virus", "Worm (gusano)" y "Trojan (troyano)" y otras como "Rootkit", "Logicbomb (bomba lógica)" y "Spyware".

31 *Ibídem*, pág. 175.

32 Mayer Lux, Laura, *op. cit.*, pág.175.

El mecanismo de operación en estos casos es el siguiente:

> en el primer supuesto, lo usual es que la página fraudulenta figure al comienzo de los resultados de búsqueda –que es donde normalmente se posicionan las páginas auténticas– y que esa misma circunstancia lleve a que la víctima elija dicha página entre todos los resultados arrojados. En el segundo supuesto, en cambio, puede que aparezca directamente la página web fraudulenta, o bien, que se abra una ventana en el navegador del usuario con la página falsa.[33]

En ambos supuestos se prevé que el usuario pueda caer en el error, por el desconocimiento de las diversas propiedades del contenido de una página, o por el contrario se cerciore de que efectivamente es una página segura ya que cubre con todos los parámetros de confiabilidad, sin embargo, se trata de una página fraudulenta.

En este delito han existido nuevas modalidades de comisión, "como la instalación de *malware* con la sola visita de la página *web* fraudulenta de que se trate".[34]

La autora menciona que muchas veces el "*phishing* y el *pharming* se presentan unidos, por ejemplo, cuando se envía a la víctima un correo spam, que contiene un link, y se le conduce a una página web que emula la del banco respectivo. Además, el empleo de un *malware* puede provocar que el *phishing* y el *pharming* se confundan en la práctica, *v. gr.*, si el *software* malicioso se utiliza para imitar una página *web*, a la que es dirigida la víctima, y desde la que se obtienen sus datos personales y bancarios. Por lo mismo, las medidas informativas y preventivas de las entidades bancarias suelen referirse a ambos supuestos, conjuntamente".[35]

Con esto podemos ver, la existencia de una serie de actividades ilícitas que ocasionan un perjuicio al usuario de los sistemas financieros, y donde el Estado debe salvaguardar el patrimonio de la población.

---

33 *Ídem.*
34 *Ídem.*
35 *Ídem.*

Existen actualmente diferentes circunstancias globales que permean en la dinámica de protección y seguridad de los usuarios de los servicios financieros, entre ellas nos encontramos la contingencia sanitaria ocasionada por el *Covid-19,* en la que hemos tenido que llevar a cabo las actividades cotidianas mediante el uso de las TIC, de manera exponencial, lo que desde luego trae consigo una mayor vulnerabilidad en la utilización de estas herramientas tecnológicas.

En este contexto la revista *IT Masters Mag* estableció en su publicación "El estado de la seguridad IT en 2020: Las superficies de ataque se amplían y las personas nunca fueron tan importantes para la defensa, que las actividades con mayor riesgo cibernético generados por la crisis Covid-19 incluyen el trabajo remoto y las compras en línea, dos tendencias que se aceleraron exponencialmente".[36]

Los directores *IT y de Seguridad* tuvieron que reaccionar tan rápido que dejaron muchas puertas abiertas, usuarios desprotegidos y sitios web mal preparados para el pico en la demanda. Ahora están percibiendo las señales de alarma y, en esta nueva etapa, deberán volver la atención a los detalles de protección de datos, control de identidad y acceso, establecimiento de nuevas políticas de seguridad y revisar su portafolio de aplicaciones con lupa. Durante la peor etapa de la pandemia, el comercio electrónico se convirtió en el único medio de acceso a múltiples productos. Personas que no se atrevían a hacer una compra en línea, en menos de dos semanas dejaron de desconfiar. De acuerdo con datos de *ACI Worldwide Research*, las ventas electrónicas del *retail* alcanzaron en algunas semanas crecimientos de 209% año contra año a nivel global. La iniciativa Covid-19 *Commerce Insight*, detalla que en México este crecimiento ha sido de 152%

36 Holloway Christopher, *El estado de la seguridad IT en 2020: Las superficies de ataque se amplían y las personas nunca fueron tan importantes para la defensa*, *https://itmastersmag.com/informes-whitepapers/el-estado-de-la-seguridad-it-en-2020-las-superficies-de-ataque-se-amplian-y-las-personas-nunca-fueron-tan-importantes-para-la-defensa/*, fecha de consulta 28 octubre 2020.

en las últimas semanas. Esta bonanza ha hecho crecer también el número y el tipo de fraudes realizados. Una herramienta diseñada por *Sift* que rastrea los eventos fraudulentos intentados y exitosos en el comercio electrónico semana a semana, reveló un aumento del 34% en ataques desde el comienzo de la pandemia. Los fraudes de No-Pago/No-Entrega, en los que se manipula al comprador para que realice la transacción sin la intención de enviarle los productos, (o viceversa, se falsea el pago para que los productos sean enviados) son el segundo tipo de ataque más popular de acuerdo con el *Internet Crime Complaint Center*, con más de 61,000 víctimas.[37]

IX. CONCLUSIONES

Con lo hasta ahora analizado, es posible pensar en algunos puntos importantes de los retos y políticas que en materia de ciberseguridad deben implementarse en el sistema financiero a través de la implementación de políticas públicas que sean congruentes con las consecuencias de la vulnerabilidad que el uso de las TIC presentan para los usuarios de estos servicios financieros en la red; algunas de estas se enumeran a continuación:

1. Garantizar el acceso a Internet a todos los sectores de la población.
2. Fomentar el conocimiento de los mecanismos de protección de la información, en todos los sectores de la población, a través de programas preventivos y de divulgación.
3. Proteger a los usuarios en la red, a fin de que cuenten con los mecanismos mínimos de una navegación segura en las plataformas financieras.
4. Seguimiento a las tendencias criminológicas de los *ciberdelincuentes*, con la finalidad de hacer congruentes las estrategias de protección con los avances tecnológicos y sus vulnerabilidades.
5. Mantener procesos de estudio permanente en el sector financiero, incluso creando redes de colaboración internacional, en materia de

37 *Ídem.*

capacitación, detección y cumplimiento de las medidas de seguridad y protección, frente a los diversos actos delictivos que se dan a través de las TIC.

6. Homologar los diversos cuerpos normativos que regulan la actividad financiera en México, para brindar mecanismos y herramientas legales que hagan más eficaz y eficiente el uso de las TIC en las diversas plataformas financieras.

XI. FUENTES DE CONSULTA

Bibliografía

Lassalle, Ferdinand. ¿Qué es una constitución?, Vigésima Edición, Coyoacán Editores, traducción de W. Roces Suárez, impreso en México, 2017.

Mendez Morales, José Silvestre. *Problemas económicos de México y sustentabilidad*. Séptima edición, 2012, Mc Graw Gill, México.

Ruiz Torres, Humberto. E*lementos de derecho bancario*. Editorial Mc Graw Hill, México.

Villanueva, Ernesto y DIAZ Vanessa. *Derecho de las nuevas tecnologías. En el siglo XX derecho informático"*, Editorial Oxford, México, año 2015.

Hemerografía

Banca mexicana acelera hacia lo digital. Nota del día 20 de marzo de 2019. Fecha de consulta 01 de septiembre de 2019. *https://www.eleconomista.com.mx/sectorfinanciero/Banca-mexicana-acelera-hacia-lo-digital-20190320-0036.html*

Educación Financiera. CONDUSEF, fecha de consulta 01 de septiembre de 2019. *https://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/educacion-financiera/763-que-son-las-fintech*

Leyva Jeanette, "Falla en data center genera caos en el uso de tarjetas en México", periódico *el financiero*. Publicación del 10 de agosto de 2019. Nota consultada 01 de septiembre de 2019. *https://www.elfinanciero.com.mx/economia/falla-en-data-center-genera-caos-en-el-uso-de-tarjetas-en-mexico.*

S/A "Hackers detrás de ataques al SPEI, estuvieron dentro de las redes de los bancos por año y medio ", periódico *el Economista*. Publicación 07 abril 2019. Nota consultada el día 01 septiembre de 2019. *https://www.eleconomista.com.mx/sectorfinanciero/Hackers-detras-del-los-ataques-al-SPEI-estuvieron-dentro-de-las-redes-de-los-bancos-por-ano-y-medio-20190407-0018.html*

Holloway Christopher, *El estado de la seguridad IT en 2020: Las superficies de ataque se amplían y las personas nunca fueron tan importantes para la defensa*, *https://itmastersmag.com/informes-whitepapers/el-estado-de-la-seguridad-it-en-2020-las-superficies-de-ataque-se-amplian-y-las-personas-nunca-fueron-tan-importantes-para-la-defensa/*, fecha de consulta 28 octubre 2020.

Mayer Lux, Laura, *Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos*, Revista Ius et Praxis, Año 24, Nº 1, 2018, *https://scielo.conicyt.cl/pdf/iusetp/v24n1/0718-0012-iusetp-24-01-00159.pdf,* pág. 163, fecha de consulta 28 octubre 2020.

Legisgrafía

Artículo 21 de la Constitución Política de los Estados Unidos Mexicanos, consultado el día 23 de junio de 2020, en *http://www.diputados.gob.mx/LeyesBiblio/pdf/1_080520.pdf.*

Cumbre Mundial sobre la Sociedad de la Información, Documento WSIS-03/GENEVA/4, Naciones Unidas, consultado en *https://www.itu.int/net/wsis/docs/geneva/official/dop-es.html*, el día 22 de mayo de 2020.

Jurisprudencia consultada el día 22 de junio de 2020 en la página *https://sjf.scjn.gob.mx/sjfsist/paginas/tesis.aspx*

Jurisprudencia consultada el día 22 de junio de 2020 en la página *https://sjf.scjn.gob.mx/sjfsist/paginas/tesis.aspx*

POLÍTICA CRIMINAL Y VIOLENCIA EN EL ESPACIO VIRTUAL

Anahy Rodríguez González*
Rodolfo Alexandro Buendía Castro**

SUMARIO: I. Introducción. II. Violencia en el espacio virtual. III. La política criminal y los espacios virtuales. IV. La justicia en tiempos virtuales. V. Conclusiones. VI. Fuentes de consulta

I. INTRODUCCIÓN

En los últimos años, hemos observado el avance vertiginoso de la tecnología, la cual ha transformado la forma en que interactuamos; un mundo real y un mundo creado, un espacio virtual a través del cual vamos desarrollando un perfil, individual y colectivo que nos permite establecer relaciones, en función de las afinidades, las expectativas, las diferencias y los límites.

La interacción entre los miembros de un grupo que buscan una satisfacción recíproca de sus necesidades –físicas, afectivas o emocionales– se ha trasladado al espacio de las redes sociales digitales, lo que refleja gráficamente la coordinación mutua

---

* Licenciada y Maestra en Derecho por la UNAM, Licenciada en Psicología por la Universidad Autónoma Metropolitana, Doctora en Derecho por la Fes Acatlán, UNAM. Es académica de tiempo completo en la Licenciatura en Ciencia Forense, de la Facultad de Medicina de la UNAM. Ha sido profesora del Posgrado en Derecho de la UNAM, en las materias de Sociología del Derecho, Criminología, Victimología y Delincuencia Juvenil. Ha impartido cursos de formación en materia de Derechos Humanos en la Universidad del Ejército y la Fuerza Aérea y en la Universidad Anáhuac del Norte. Y ha dirigido tesis de licenciatura y maestría en el área de la criminología, los derechos de las víctimas y la política criminal.

** Licenciado y Maestro en Derecho por la por la UNAM, cuenta con un Máster en Derecho Medioambiental y Sostenibilidad por la Universidad de Castilla-La Mancha, actualmente es estudiante del tercer semestre del Doctorado en Derecho por la UNAM. Es Profesor en la Universidad del Ejército y Fuerza Aérea Mexicana donde imparte las materias de Derechos Humanos y Derecho Internacional Humanitario, además de impartir clases en la Universidad Anáhuac del Norte.

representada en vínculos, que a diferencia de los creados en la interacción física o personal, no resultan siempre tan afectivos o profundos; pero que generan la ilusión de no estar solo, siempre acompañado por la mirada de ese gran *Otro* que se convierte en alguien difuso, sin corporeidad, pero con una presencia permanente. Aunado a esto, la imagen del mundo libre que parece representar el mundo virtual choca con la rigidez institucional y social del mundo real, el cual esta atravesado por reglas y pautas de comportamiento.

De esta forma, la interacción social se acelera al ritmo del avance de los diversos dispositivos tecnológicos, la creación de aplicaciones que van inventando nuevas formas de comportamiento social o bien, llevando las ya existentes a modalidades que imponen modas, pautas de relación y definición de nuestro lugar dentro del espacio virtual. Así, las redes sociales digitales van construyendo un mundo paralelo, que refleja los conflictos y estructuras presentes en la vida "real" y con ello, la aparición de problemáticas sociales como la desigualdad, las vulnerabilidades, la racialización y la interseccionalidad de las violencias; van manifestándose en la medida en que nuestra interacción aumenta. De esta forma: "La cultura, en su forma moderna, incita el odio contras las convenciones y virtudes de la vida cotidiana, que ha llegado a racionalizarse bajo las presiones de los imperativos económicos y administrativos."[1]

Los conflictos que se encuentran presentes de manera natural en la vida de todo ser humano y su capacidad para *negociar* y resolver esas diferencias se ponen en práctica en un espacio que se construye vertiginosamente, cuyas reglas se inventan en función de la oferta y la demanda, del producto final que constituye ese ser interconectado.

En consecuencia, las bondades y los riesgos que ha traído consigo el uso de tecnologías de la comunicación y de aparatos tecnológicos inteligentes, que nos permiten estar interconectados, generan el surgimiento de diversas conductas transgresoras, que en

1 Habermas, Jürgen, et. al., La posmodernidad, Editorial Kairós, Barcelona, España, 2006, p. 24.

muchos casos comienzan a ser tipificadas por los diversos sistemas jurídicos; con la intención de proteger a las personas, ahora en su esfera virtual.

Sin embargo, un tema controversial es el relaciona con el alcance de las limitaciones jurídicas que el Estado puede o debe imponer a los usuarios de estos espacios, cuestionando cuándo nos encontramos ante una protección y cuando ante una posibilidad de establecer mecanismos de control estatal que limiten el ejercicio de la libertad de expresión; además de llevarnos a reflexionar respecto del papel que ejercemos, como usuarios de las redes sociales virtuales, en el ejercicio de la violencia y los mecanismos para su prevención; tema que será abordado en este artículo.

II. VIOLENCIA EN EL ESPACIO VIRTUAL

La ‹*violencia*› es entendida como el acto intencional a través del cual, por medio de la fuerza física, psicológica o moral; se busca causar un daño a otro o limitarlo en su libertad. La violencia entonces opera dentro de un contexto determinado por el sujeto que la ejerce y tiene como función sacar a otro de su estado natural, con la finalidad someter o dominar su voluntad. Debido a lo anterior, la violencia es considerada como un fenómeno interseccional, es decir, aquella que tiene orígenes en diversas estructuras, fundamentadas en la desigualdad y la vulnerabilidad y que, se presenta de formas diversas dentro de la dinámica social, por lo que obedece a un contexto histórico determinado y es un hecho continuado que busca potencializar sus efectos.

En consecuencia, el análisis del fenómeno de la violencia deberá contemplar una investigación del psiquismo individual y las instituciones sociales producto de esos individuos, para establecer qué tipo de sistema es al que pertenecemos, un sistema social basado en la convivencia de unos con otros o bien sistemas jerárquicos o de poder que se definen como: “sistemas de convivencia constituidos

bajo la emoción que constituyen las acciones de autonegación y negación del otro, en la aceptación del sometimiento propio o del otro en una dinámica de orden y obediencia."[2] Y que de presentarse esta última situación, no serán considerados sistemas sociales propiamente dichos.

El ejercicio de la violencia implica en primer lugar, la creación del arquetipo del adversario y sobre el cual se proyecta la sombra del grupo. En segundo lugar, necesita una sociedad en la que no se tolera el concepto de igualdad. Requiere de sujetos dualistas, donde la posibilidad de lo diferente es impensable. Esa justificación ideológica que se construye del diferente es la base sobre la cual se erigen el conjunto de acciones violentas ya sea en el ámbito de lo público, de lo privado o en este caso, de lo virtual; de un ejército contra sus ciudadanos, de un padre contra su hijo o de sujetos virtuales que imponen una tendencia respecto de la construcción de la realidad que hacen a partir de una percepción impuesta y manipulada.

De acuerdo con Ignacio Martín-Baró, en su obra *Acción e Ideología*,[3] la violencia tiene cuatro elementos constitutivos: la *estructura formal del acto*, la *"ecuación personal"*, el *contexto posibilitador* y el *fondo ideológico*.

En primer lugar, la *estructura formal del acto* refiere que el suceso de violencia se caracterice por la aplicación excesiva de la fuerza sobre una persona, organización o proceso. En este punto el autor señala que este elemento sirve para diferenciar los *actos de violencia terminal* de los *actos de violencia instrumental*. En los actos de violencia terminal el fin que se persigue es el efecto inmediato de la violencia, el acto violento en sí mismo, ejemplos de este son la muerte de un individuo, la violación de una mujer o el linchamiento mediático en redes sociales. En los actos de violencia instrumental, el uso excesivo

---

2 Maturana R, Humberto, *Desde la Biología a la Psicología*, Editorial Lumen, Argentina, 2003, p. 97.

3 Martín Baró, Ignacio, *Psicología social desde Centroamérica*, Editorial UCA, El Salvador, 2004, p.372

de la fuerza es un medio que permite alcanzar un objetivo distinto, por ejemplo, la tortura para obtener una confesión, el asesinato de un adversario político para poder ocupar un puesto político o la creación de noticias falsas que cambian la percepción de las personas respecto de un tema o situación.

El segundo elemento se refiere a la *ecuación personal*, con lo que se pretende estudiar las características individuales del sujeto que lo realiza, es decir, aquellas acciones violentas que son atribuibles a las características individuales del sujeto. Este elemento es de interés para el estudio de la violencia en espacios virtuales, ya que, a través del análisis de la ecuación personal es posible visibilizar las estructuras que generan vulnerabilidades, desigualdad y limitaciones en el ejercicio y goce de derechos en ciertos grupos. Por ejemplo, pensemos en la construcción de categorías como *"fifi"* y *"chairo"*, que en uno y otro sentido, ponen en evidencia características atribuidas que parecen justificar ataques discursivos en redes sociales y esa justificación refuerza la idea del enemigo de la que se hablo en párrafos anteriores, reduciendo el dialogo al enfrentamiento de opuestos sin que puedan construirse espacios de comunicación efectiva.

El tercer elemento consiste en el *contexto posibilitador*, en el cual es factible que se lleve a cabo el acto de violencia pues se encuentran las condiciones propicias para ello. En este punto, el autor identifica dos tipos de contextos: el social y el situacional. En el caso del contexto social, la presencia de violencia es consentida de manera explícita o implícita en los valores o normas que regulan las relaciones entre los sujetos que conforman el grupo. Así podemos decir que: "En la medida en que este contexto se encuentre institucionalizado, es decir, convertido en normas, rutinas y medios materiales, la violencia podrá alcanzar cotas mayores."[4] El contexto situacional hace referencia al entorno personal, en el que los individuos se

4 *Ibidem*, p.374.

desarrollan y van construyendo su percepción del mundo; por lo que, este se construye a través de las experiencias de vida, las dinámicas familiares, los modos de crianza, la vida comunitaria, entre otros aspectos.

La importancia del contexto, en el tema de la violencia en espacios virtuales, radica en que es una mirada a la dinámica de interacción de una sociedad, manifestando de forma más evidente sus valores, la capacidad empática entre sus miembros, sus procesos civilizatorios, su respeto por las normas, y la capacidad de diálogo; en sentido contrario, la ausencia de esto se manifestará en conductas innovadoras y trasgresoras en la dinámica virtual, con posturas polarizadas que acentuarán las desigualdades y carecerán de reflexión sobre la vida social.

El cuarto y último elemento de la violencia es su *fondo ideológico*, es decir, las construcciones discursivas que determinan su justificación. Estos discursos de poder definen la forma en que la realidad social e institucional se va conformando; en el caso de la realidad virtual, la manipulación de la percepción, a través de un bombardeo de información, en la que las personas no son capaces de discernir efectivamente la veracidad de los datos proporcionados es esencial, pues permite un efectivo control social y por lo tanto, un ejercicio de poder discrecional.

Por último, es necesario señalar que los espacios en los que la violencia se manifiesta son diversos y producen efectos variados sobre los individuos que se ven afectados por ella. La identificación de cada uno de esos contextos resulta indispensable para la determinación de las responsabilidades, que deberán fincarse en los actores de la comisión de actos que violentan la integridad de diferentes participantes. En el caso de las redes sociales digitales o los espacios virtuales, este es un tema de gran interés para la política criminal, pues la prevención de conducta delictivas se enfrenta a la rapidez de la evolución de la realidad virtual *versus* la realidad y los tiempos establecidos para la construcción de las normas.

Actualmente, la trivialización de conceptos como violencia, derechos humanos y abuso de poder, ha generado su uso indiscriminado y una confusión en la tipificación de delitos que se cometen en los espacios virtuales. Sin embargo, es importante recordar que la violencia está presente en todo el tejido social, sin embargo, los ámbitos en los que se desarrolla revisten importancia en el contexto jurídico pues constituyen los parámetros que se emplean para determinar responsabilidades, tipificar delitos y abrir espacios institucionales para el acceso a la justicia. En el caso de la violencia en espacios virtuales, su análisis debe atender a dos aspectos esenciales: la protección de la libertad de expresión, sin que esto excluya la identificación de las formas delictivas novedosas y la consecuente protección de quiénes se ven afectados en su esfera jurídica.

Byung-Chul Han nos dice que la violencia, en la actualidad: "muta de visible en invisible, de frontal en viral, de directa en mediada, de real en virtual, de física en psíquica, de negativa en positiva, y se retira a espacios subcutáneos, sub comunicativos, capilares y neuronales…"[5]

Así, la violencia que generalmente tiene un agente activo (quien ejerce la violencia) y uno pasivo (quien la sufre) se transforma en los espacios virtuales, en los que los agentes, especialmente los activos, se desvanecen. El acto violento, en la virtualidad se genera y se replica a escalas geométricas de redes; se aprecia por sus efectos, pero su origen se pierde.

El acto violento virtual aparece y lo compartimos con una facilidad; se trata solo de tocar una pantalla o apretar un botón y el acto se reproduce infinitamente; no hay tiempo para reflexiona si lo compartido lesiona a alguien, se comparte porque se es parte de una comunidad digital, en la cual, si no se participa no hay existencia. La identidad virtual es una extensión del yo, en el que

5 Han, Byung-Chul, *Tipología de la Violencia,* Herder, 2016, Barcelona, p. 6

la percepción, la tendencia y las afinidades se transmiten al teclear. Así twitteamos y luego existimos.

III. LA POLÍTICA CRIMINAL Y LOS ESPACIOS VIRTUALES

De acuerdo con Moisés Moreno Hernández, la Política Criminal es: "una manifestación del poder que tiene el Estado para enfrentar un fenómeno que es la delincuencia como parte de la política social (general) del Estado, por lo que está o debe estar acorde con dicha política general y acomodarse a las exigencias del tipo de Estado de que se trate".[6] En otras palabras, la política criminal es el mecanismo a través del cual, el Estado busca la prevención del fenómeno delictivo a través de diversos medios -educativos, normativos, institucionales, axiológicos, entre otros- , en consonancia con la estructura de poder y organización de que se trate.

En congruencia con lo anterior, podemos visualizar dos situaciones que estudia la política criminal: el primero, el poder del Estado para enfrentar el fenómeno de la delincuencia y, por otro lado, el hecho de que la política criminal sea considerada parte de la *política social general* del Estado.[7]

Actualmente, existen en México diversos problemas que son objeto de interés de la política criminal; uno de ellos es la evolución de los espacios virtuales. En el año 2019, las cinco redes con mayor importancia en porcentaje de usuarios fueron las siguientes: Facebook con 99%, WhatsApp con 93%, YouTube con 82%, Instagram con 63% y Twitter con 39%[8]; en este sentido,

---

6 Moisés Moreno Hernández, "Función e importancia de la Política criminal", en *Revista de Política Criminal y Ciencias Penales,* Cepolcrim, agosto, núm. Especial 1, México, 1999, p.128.

7 Manuel Vidaurri Aréchiga, *Bases generales de criminología y política criminal*, 1ª Edición, Oxford University Press México, México, 2017

8 Statista, 2020 https://es.statista.com/estadisticas/1035031/mexico-porcentaje-de-usuarios-por-red-social/ fecha de consulta 19 de agosto 2020

es innegable el efecto que estos espacios virtuales generan en las personas al imponer tendencias que nos *"obligan"* a pensar de cierta forma, establecer pautas de interacción e incluso desviar nuestra atención de problemas esenciales de nuestra vida cotidiana para enfrascarnos en conflictos construidos a partir de percepciones.

Un desarrollo en la tecnología. que en principio vislumbraba bondades y ventajas del acceso a la información de forma inmediata, ahora han evolucionado en una especie de amenaza persistente sobre nuestra identidad.

Ahora bien, desde hace por lo menos ocho años, el gobierno mexicano, ha propuesto diversos tipos de controles en los espacios virtuales, los cuales no han fructificado, quedando en intentos e iniciativas. Ante la dificultad de controlar un espacio de información ilimitada, se han generado lineamientos oficiales, que buscan regular el papel de los funcionarios públicos en las redes sociales, limitando el control no al espacio, sino al sujeto que lo emplea; un ejemplo de esto son los lineamientos oficiales conocidos como las Políticas Generales para la Difusión de Información Pública mediante Redes Sociales Digitales, provenientes del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.[9]

En este documento, conforme a las fracciones VIII y X, de la disposición Primera, se señala que estas políticas tienen como finalidad:

> …
> VIII. Brindar certeza a la sociedad sobre cuáles son las cuentas de redes sociales administradas por los sujetos obligados y establecer una definición para los tipos de cuentas de redes sociales digitales usadas para difundir información pública,
> X. Establecer recomendaciones y buenas prácticas a los sujetos obligados respecto a la utilización y manejo de las redes sociales digitales como mecanismos para la difusión de información pública.

9 CONAIP/SNT/ACUERDO/EXT01-18/06/2019-03

De las fracciones previamente citadas, podemos inferir que hay un control para brindar seguridad a la población sobre la información a la que accede, tener certeza de quien la escribe y orientar a los funcionarios titulares de redes sociales a difundir información pública y verídica, con la intención de tener clara la relación que existe entre la información publicada y la responsabilidad que tiene él que la digitaliza y hace de conocimiento popular.

Este argumento que se robustece con lo establecido en la segunda parte de dichas políticas, en su fracción III dónde se define que:

> Cuenta personal de servidor público: Cuenta privada de red social digital que es creada y administrada directamente por un servidor público sin recibir ningún tipo de recursos públicos para su administración o difusión, en la que voluntariamente dicho servidor público ha decidido difundir información y actividades derivadas de su cargo, de la que procurarán respaldar dicha información en los archivos del sujeto obligado, independientemente del soporte documental y conforme a las regulaciones aplicables en la materia.[10]

Por esta razón, es posible ver leyendas, principalmente en cuentas de *Twitter*, del siguiente estilo: *cuenta personal, opiniones a título personal*; para establecer que, aun cuando se trate de una cuenta privada, el servidor público debe hacerse responsable de la información, opiniones y datos que trasmite a través de ella.

De esta forma, el titular de la cuenta quedará como responsable de su cuenta, de su información y de su contraseña: "*La administración y contraseñas de acceso a este tipo de cuentas personales son ajenas al sujeto obligado, pues el titular de los derechos de dicha cuenta es el servidor público como* ***física*** *y podrá continuar utilizando y administrando la misma cuando concluya su cargo público.*"[11]

Si bien, estas políticas generales hacen referencia a la difusión de información pública y la obligación de cuidar la verdad de lo

10 *Idem*.
11 *Idem*.

que se hace público, es posible observar un mecanismo de control del Estado en materia de redes sociales, en espacial en el aspecto económico, al disponer de partidas para la gestión de las mismas a través de los llamados *community manager,* al señalar si se puede o no seguir siendo titular de la contraseña de una cuenta personal de redes sociales digitales o, en el caso de que se trate de una cuenta Institucional, definir el manejo de las contraseñas y su cambio al ser entregadas por el servidor público a través de actos formales como son las actas de entrega recepción.

Otro ejemplo de un mecanismo de política criminal es el desarrollo de la política de protección al usuario de Internet, a través de la creación de la *Policía de Ciberdelincuencia Preventiva*, la cual tiene principalmente 3 líneas de acción[12]:

1. Monitoreo de redes sociales y sitios web en general
2. Pláticas informativas en centros escolares e instituciones de la Ciudad de México, con el objetivo de advertir los delitos y peligros que se cometen a través de internet, así como la forma de prevenirlos, creando una cultura de autocuidado y civismo digital.
3. Ciberalertas preventivas las cuales se realizan a través del análisis de los reportes recibidos en las cuentas de la Policía de Ciberdelincuencia Preventiva.

Esta policía opera los 365 días del año, las 24 horas del día, monitoreando diversas conductas delictivas en los espacios digitales como son:[13]

1. Insultos electrónicos, ofensas que algún o alguna usuaria hace a otra u otro.
2. Hostigamiento, implica el envío de mensajes ofensivos de forma reiterada a una persona determinada, ya sea por medio del correo

12 Secretaria de Seguridad Pública, 2020, http://data.ssp.cdmx.gob.mx/ciberdelincuencia.html fecha de consulta 15 de agosto 2020.

13 Secretaria de Gobernación, 2020, https://www.gob.mx/conavim/articulos/has-sufrido-acoso-cibernetico-te-decimos-a-donde-acudir fecha de consulta 11 de agosto 2020

electrónico, chats, mensajes de texto, etc.

3. Denigración, se refiere a la difusión de información despectiva o falsa de alguna persona, como es el caso de la publicación de fotografías alteradas.
4. Suplantación, implica que el o la acosador se haga pasar por la víctima, ya sea utilizando la contraseña de acceso de sus cuentas online para enviar mensajes agresivos u ofensivos o terceras personas como si hubieran sido enviados por la propia víctima.
5. Sonsacamiento, radica en revelar información privada de la víctima que en un principio fue enviada por la víctima de forma privada o sonsacada para después difundirla a otras personas sin permiso de la víctima
6. Exclusión, se realiza con la finalidad de excluirla o no dejarla participar.
7. Ciberpersecución, consiste en el envío de comunicaciones electrónicas reiteradas hostigadoras y amenazantes
8. Happy slapping, en la cual se realiza una agresión física que se graba por algún medio digital para ser publicado en la red y sea público.

De esta forma, las construcciones de conductas típicas que representan una afectación a la esfera jurídica de las personas en el ámbito digital van estableciendo mecanismos de intervención para su detección oportuna, su castigo y la prevención a partir de la divulgación de estas a la población en general.

1. Otros ejemplos de control sobre el espacio virtual

a) Ley "Antimemes"

Esta iniciativa de ley fue impulsada por la diputada federal Nayeli Salvatori, del Partido Encuentro Social, después de subir un video a su cuenta en la red social denominada Tik tok (@naysalvatori), en el que hace una imitación, con una canción de fondo, en la que se escuchan sonidos de balazos mientras ella estaba ubicada en el Salón del Pleno del Congreso de la Unión. Dicho video fue editado por un medio local y poco después, la diputada expresó que había

recibido amenazas, situación que la motivo a crear la iniciativa y presentarla en un video en el que señalaba: "*es una reforma al Código Penal Federal, que si tú modificas el contenido original de algo: una fotografía, un video o un audio, bueno pues serás castigado y además se va a proponer en la Comisión de Radio y Televisión, que a través del Instituto Federal de Telecomunicaciones (IFT), voy a proponer que esa cuenta, en lo que se hacen las investigaciones pertinentes, la cuenta sea dada de baja*"[14].

En videos subsecuentes, en los que se le preguntó si se permitiría seguir haciendo "memes", que de acuerdo con el Diccionario de la Real Academia de la Lengua Española[15], se define como la imagen, video o texto, por lo general distorsionado con fines caricaturescos, que se difunden principalmente a través de internet; ella contesta: "*al parecer pasaré toda mi vida aclarando esto, nadie prohibió los memes, es que solamente leen el encabezado y no la letra completa y por eso el país está tan ignorante (sic), no se trata de eso, se trata de, te voy a dar un ejemplo, tu sales en una foto sentado y en una mesa al frente y yo edito la foto y le pongo cocaína y la subo en redes y pongo este wey es un pinche coco, lo hago viral y te daño en tu trabajo, en tu familia, tu vas a tener la oportunidad de demostrar que esa foto era falsa, pelear, denunciar y así evitar que dañen tu buena honra, de eso se trata, puedes seguir haciendo memes, por Dios, tenemos un país bien ignorante porque nada mas creen lo que dicen los medios, investiguen, métanse a los dictámenes, de verás, no funciona así, aparte tendrías que denunciar, fiscalía tendría que hacer un análisis, una investigación y ya de ahí se vería si hay un culpable o no, por Dios, lean*".15

Derivado de esta ultima participación, la controversia aumentó y finalmente la iniciativa no prosperó; sin embargo, se abrió un debate sobre la necesidad de establecer límites sobre lo que es posible y lo que no, dentro de los espacios de las redes digitales y cómo estos límites pueden afectar la libertad de expresión.

---

14 S/A, "Presentarán Ley Antimemes", del periódico *EL UNIVERSAL*, 2020, https://www.eluniversal.com.mx/nacion/diputada-del-pes-presentara-ley-antimemes-castigara-modificaciones-en-redes-sociales fecha de consulta 12 de agosto 2020.

15 Diccionario de la Real Academia de la Lengua Española, 2019, https://dle.rae.es/meme, fecha de consulta 25 de septiembre de 2020.

b) Lady Censura

En las redes sociales digitales se ha vuelto común denominar a alguien que es grabado haciendo algo indebido, ilegal o simplemente absurdo[16] con el sobrenombre de *Lord,* si es masculino o *Lady,* si se trata de una mujer. Esté tema que parece trivial, causó controversia en el ámbito político después de que la diputada María Rosete Sánchez, del Partido Encuentro Social, presentara una iniciativa de Ley para evitar el uso de dichas etiquetas.

La Diputada planteó en su iniciativa la reforma a varios artículos de la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, para incluir el término de en violencia digital, toda vez que este tipo de etiquetas pueden causar daño psicológico, emocional, sexual, patrimonial o de índole social a mujeres y hombres. [17]

Esta propuesta nuevamente fue ampliamente discutida pues aborda dos elementos que son motivo de controversia: la regulación vista como un intento de censura a la libertad de expresión y la protección de la integridad de las personas que son objeto del escarnio social a través de estos estereotipos. Además, pone énfasis en la presencia de acciones de violencia dentro del espacio digital, por lo que se trata de temas de alto interés para la política criminal y lleva la reflexión hacia el papel de las redes sociales como un medio para visibilizar situaciones, en las que una persona o grupo de personas, transgreden el estado de derecho, logrando una prevención general negativa a través de la intimidación, no ya de la ley, sino del reproche social.

---

16 En términos del gran autor francés Albert Camus, lo absurdo nace de esa confrontación entre el llamamiento humano y el silencio irrazonable del mundo. Eso es lo que no hay que olvidar. A eso hay que aferrarse, pues toda la consecuencia de una vida puede nacer de ellos. Lo irracional, la nostalgia humana y lo absurdo surge de su cara a cara, he aquí los tres personajes del drama que debe terminar necesariamente con toda la lógica que es capaz una existencia. El mito de Sisífo, 1942.

17 Grupo Radioformula, 2020 https://www.radioformula.com.mx/noticias/20190809/diputada-propone-castigar-uso-de-lords-y-ladies-y-la-bautizan-como-ladycensura/ fecha de consulta 17 de agosto 2020

Finalmente, a partir de estos ejemplos es posible dirigir la discusión hacia el papel de las redes sociales digitales como espacios en los que una *violencia juguetona* o *lúdica*[18], que despliega una capacidad de destreza para satirizar o ridiculizar actos o circunstancias cotidianas, se va convirtiendo en una *violencia vengativa*[19] que expresa forma patológicas de interacción, que tienen como función irracional anular al otro y que convierte a la venganza en la posibilidad de autoafirmación y ejercicio de poder.

IV. LA JUSTICIA EN TIEMPOS DE LA VIRTUALIDAD

Vigilar y Castigar, de Michel Foucault inicia así:

> Damiens fue condenado el 2 de marzo de 1757, a 'pública retractación ante la puerta principal de la Iglesia de París', adonde debía ser llevado y conducido en una carreta, desnudo, en camisa, con un hacha de cera encendida de dos libras de peso en la mano', después, 'en dicha carreta, a la plaza de Grève, y sobre un cadalso que allí habrá sido levantado [deberán serle] atenazadas las tetillas, brazos, muslos y pantorrillas, y su mano derecha, …quemada con fuego de azufre, y sobre las partes atenaceadas se le verterá plomo derretido… y a continuación su cuerpo estirado y desmembrado por cuatro caballos y sus miembros y tronco consumidos en el fuego, reducidos a cenizas y sus cenizas arrojadas al viento´.[20]

En está narración, la función del suplicio es la de un espectáculo, en el que todos los asistentes son responsables del sufrimiento en el cuerpo del delincuente, pero también son participes del castigo impuesto por la afrenta cometida; se convierte en el momento en que el delincuente se encuentra suspendido de sus derechos y por lo tanto toda conducta realizada sobre él está plenamente justificada.

---

18 Fromm, Erich, El corazón del hombre, Fondo de Cultura Económico, México, 2009, p. 8

19 *Ibidem*, p. 10

20 Foucault, Michel, *Vigilar y Castigar*, Siglo XXI, trigésima quinta edición en español, México, 2008, p. 11

Ahora, analicemos el siguiente caso:

El 31 de julio del 2020, un vehículo de la ruta 83, recorría su camino en la carretera México-Texcoco y fue abordado por un presunto delincuente. Este pide a los usuarios se despojen de sus pertenencias y se las entreguen. La escena parece cotidiana, una de tantas que ocurren diariamente a quienes se trasladan en el transporte público del Estado de México hacia la capital; sin embargo, en esta ocasión el chofer de la combi acelera, por lo que el compañero del presunto delincuente no logra subir al transporte y lo deja solo, cuando este intenta bajarse, es bloqueado por la persona que se encuentra sentado cerca de la puerta e inmediatamente al ver al sujeto desarmado y sorprendido, los pasajeros se abalanzan contra él y lo tunden a golpes por aproximadamente cuatro minutos; el transporte se detiene y los pasajeros enfurecidos le quitan el pantalón en la vía pública, dejando al presunto delincuente tendido en el asfalto. Todo lo anterior fue grabado y rápidamente el video se viralizó en redes sociales.

¿Qué paralelismos encontramos entre la ejecución pública de un regicida de mediados del siglo XVIII y la humillación pública de un presunto delincuente en el siglo XXI? Más allá de las obvias diferencias, hay una significación simbólica: no solo son ejemplos de justicia retributiva, sino que ejemplifican una justicia espectacular, una justicia hecha para ser vista.

Imaginemos al enardecido espectador de la ejecución en la Plaza de *Grève*, sus gritos enloquecidos lo hacen olvidar la miseria en la que transcurre su vida; ahora, comparémoslo con el cibernauta absorto frente a su pantalla, que ve una y otra vez el video del del presunto delincuente de la ruta 83, tecleando comentarios que lo hace parte de la sanción y el escarnio social.

La ejecución, lo ocurrido en el caldaso público transcurría en un solo momento, pasado el cual, sólo quedaban los testimonios de quienes lo presenciaron; en tanto que, en el caldaso virtual del que hablamos, la sanción puede ser reproducida una y otra vez;

quedando fija en la realidad virtual y manipulada las veces que el espectador desee. El espectador virtual participa de la sanción en cada reproducción, cada vez que comparte la imagen sin que haya estado presente en el lugar y en el momento en que los hechos suceden, así, a través de la pantalla, se apropia de una realidad de la cual no tiene más certeza que lo que observa.

Pero lo más importante no está del lado del espectador sino de quién da el espectáculo, el poder de dirigir las miradas del espectador ya no es exclusivo del Estado, se ha desplazado hacia quien puede grabar un video y difundirlo en redes sociales, se ha desplazado hacia prácticamente cualquier persona. Se trata de una acción potencializadora de "justicia" que se transforma en venganza ante el vacío que deja el Estado en su papel de procurar justicia, garantizar la seguridad jurídica y el estado de derecho.

Esta espectacularidad, asincronía, la viralización espacial y el anonimato a través del cual se ejerce está justicia virtual, parece estar transformando las relaciones de poder, transformando el espacio digital en una especie de panóptico virtual con el que se ejerce la vigilancia y el castigo como forma de control social.

En ese sentido, las redes sociales tienden a cambiar los puntos de equilibrio de poder, el cual es medido por el número de seguidores, las tendencias (basadas en la viralización de contenidos) y la capacidad de los usuarios de imponer percepciones específicas sobre la "realidad" y parece dejar claro que, al menos hasta el momento, las leyes han sido inútiles para regularlas. Casos como el de la Ley Antimemes o la Lady Censura nos muestran que la inercia de los actores institucionales, ante problemas como la violencia en los espacios virtuales, es esencialmente reactiva, basada en la prohibición; sin embargo, este cambio en la correlación de fuerza hace que la sociedad de la era digital reacción en el mismo espacio con fuerza.

Pero hay razones más profundas para la inutilidad de las leyes en la regulación del comportamiento digital de los individuos: los

órganos del Estado captan realidades que identifican como espacios necesarios de intervención normativa; de esta forma, generalizan y abstraen estas realidades en proposiciones hipotéticas del tipo: si sucede a, debe aplicarse b; con lo que pretenden modificar el estado de cosas que dio lugar a esa la realidad virtual. No obstante, el problema se centra en el hecho de tratar de regular un espacio no real, abstracto y sumamente dinámico; y en ese sentido, cualquier intento de encerrar en una proposición hipotética un estado de cosas virtuales se encontrará con que ese espacio evolucionó de manera acelerada, haciendo imposible la definición hipotética en la ley.

1. La Ley Olimpia, un ejemplo de política criminal en el espacio digital.

Los espacios virtuales han demostrado el beneficio de la interconectividad y el acceso a la información de forma libre y variada; además, han permitido la exposición mediática, a gran escala, de diversos fenómenos violentos, como lo es la violencia de género.

México es uno de los países con mayor índice de violencia contra las niñas y las mujeres. Desde el año 2007, la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia[21] ha definido las diversas formas en que esta violencia se manifiesta, desde la violencia física hasta la violencia feminicida, que ha obligado a la reforma de códigos penales que contemplen delitos como el *feminicidio.* Al ser el espacio virtual un reflejo de las dinámicas sociales en la realidad física es de esperar que conductas relacionadas con la violencia de género encuentren formas novedosas de manifestarse.

Este es el caso de la *Ley Olimpia*, impulsada por Olimpia Coral Melo, quién en 2014, sufre la exposición de un video íntimo en

21 Cámara de Diputados del H. Congreso de la Unión, Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, http://www.diputados.gob.mx/LeyesBiblio/ref/lgamvlv.htm, fecha de consulta: 25 de septiembre de 2020

redes sociales como venganza de su expareja por haber concluido la relación. Su exigencia de castigo se vio traducida en una serie de reformas al Código Penal y a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia para castigar la llamada *porno venganza* o *sexting*, la cuál consiste en la publicación de videos o fotografías con contenido sexual hechos por el remitente, pero enviados por el destinatario a diversas personas sin su conocimiento o consentimiento, dicha situación se agravará si es que se hace uso comercial con el material; la *violación a la intimidad sexual* por divulgación de fotografías, audios o videos con contenido sexual; el *robo de material sexual,* el cual castiga el robo y divulgación del mismo; el *acoso sexual digital* que sanciona la vulneración de confianza derivada de una relación afectiva para divulgar material sexual; el *robo de material sexual y la protección a niños y adolescentes,* que busca proteger a esta población de personas que intenten obtener o enviar material con contenido sexual; el *acoso sexual en el transporte público,* que entre otras, castigará el tomar videos o fotografías sin consentimiento o masturbarse y la *violencia digital*, estableciendo la posibilidad de que dicha conducta se ejerza por medio de un correo electrónico, redes sociales e internet.

Así, La Ley Olimpia resulta ser un fenómeno jurídico de vanguardia para un mundo tecnológico y una política criminal exitosa, que busca prevenir la realización de conductas delictivas dentro de un espacio que hasta hace poco consideraba estos delitos como formas normales de interacción.

La incorporación de conductas y sanciones claras, el reconocimiento de agresores y víctimas posibilita que, si no es posible regular en su totalidad dicho comportamiento, si permite que quienes interactúan en estos espacios comiencen a respetar pautas de comportamiento y a reflexionar sobre los alcances de las acciones al momento de participar en la divulgación de información.

V. CONCLUSIONES

Es innegable que vivimos inmersos en el desarrollo acelerado de los medios digitales de comunicación. Esa dinámica condiciona que todos los ámbitos de nuestra vida se trasladen a una virtualidad que funciona como un espejo de nuestra realidad. Así, la violencia que atestiguamos en la vida diaria se ha instalado también en ese espacio virtual

En esté breve capítulo, una primera aproximación a la violencia virtual concluye que es tan real como la violencia presencial, con las mismas características, replicando los mismos elementos estructurales; de esta forma, puede ser terminal o instrumental; presenta una ecuación personal, hay agentes activos y pasivos que reflejan los desequilibrios notables de poder los contextos posibilitadores y fondos ideológicos.

La manifestación de la violencia hacia el espacio virtual ha generado paralelamente la conciencia de que, al igual que en la realidad presencial, se debe regular las interacciones y mecanismos digitales, con la intención de prevenir de forma oportuna la afectación a las esferas jurídicas de las personas y en su caso, sancionar de forma efectiva dichas conductas lesivas a fin de evitar que estás se repliquen por todo el espacio virtual.

No obstante, rápidamente nos hemos dado cuenta que la violencia digital no puede ser regulada aplicando los arquetipos de regulación tradicionales; esto es, porque tiene características adicionales que hacen que debamos adecuar nuestras formas de regulación de los fenómenos sociales. De esas características adicionales resaltamos dos: la violencia virtual es espectacular, es decir, está hecha para que otros la vean, el agente activo quiere que todo el mundo presencie el acto violento; y por otra parte, la violencia virtual se viraliza a velocidades inimaginables en el espacio presencial, lo que provoca que el acto violento se replique y la imagen del sujeto activo tienda a desvanecerse.

Por esta razón, la política criminal es la disciplina idónea para analizar y reflexionar sobre las formas, causas y efectos de la violencia en los espacios digitales; aunado a esto, representa una herramienta indispensable para la creación de políticas de prevención y persecución de las conductas potencialmente criminales que se desarrollan en ellos. Intentos como la llamada Ley Olimpia nos muestran que ante la dificultad de controlar el espacio se trata de educar al usuario con la definición de pautas de comportamiento y la incorporación de conductas y sanciones claras.

Este ejemplo permite la reflexión sobre el papel que la política criminal, implementadas por el Estado debe cumplir en la construcción de espacios virtuales más seguros, reflexivos y en su caso, sancionadores, no solo con la fuerza de la venganza, sino con el peso de las instituciones. Y permite entender, que no se trata de generar un control absoluto del espacio digital, sino de establecer parámetros de interacción que respondan al conjunto de valores que una sociedad considera necesarios en su propio proceso civilizatorio.

La era digital nos ha transformado, pero es importante recordar que: "Todos los animales que viven en grupo generan orden porque sus motivaciones coinciden."[22] Ya sea en la realidad social o en la realidad virtual, son las coincidencias las que nos permiten avanzar en la construcción de espacios solidarios y respetuosos; abiertos a las diferencias y capaces de generar la reflexión y la evolución de las personas/usuarios.

---

22 Marina, José Antonio y María de la Valgóma, *La lucha por la dignidad*, editorial Anagrama, Barcelona, España, 2005, p. 57.

VI. FUENTES DE CONSULTA

Bibliografía

Bauman, Zygmunt, *La globalización*, Fondo de Cultura Económico, México, 2011.

Camus, Albert, El mito del Sísifo, Alianza Editorial, España, 2017.

Debord, Guy, *La sociedad del espectáculo*, Pretextos, EUA, 2000.

Foucault, Michel, *La hermenéutica del sujeto*, Curso en el Collége de France (1981-1982), Fondo de Cultura Económica, Segunda Edición, México, 2012.

------- *Obras esenciales*, Paidós, Barcelona, 2013.

------- *Vigilar y Castigar*, Siglo XXI, trigésima quinta edición en español, México, 2008.

Fromm, Erich, *El corazón del hombre*, Fondo de Cultura Económico, México, 2009.

Habermas, Jürgen, et. al., *La posmodernidad*, Editorial Kairós, Barcelona, España, 2006.

Han, Byung-Chul, *Tipología de la Violencia*, Herder, Barcelona, 2016.

Marina, José Antonio y María de la Valgóma, *La lucha por la dignidad*, editorial Anagrama, Barcelona, España, 2005.

Martín Baró, Ignacio, *Psicología social desde Centroamérica*, Editorial UCA, El Salvador, 2004.

Maturana R, Humberto, *Desde la Biología a la Psicología*, Editorial Lumen, Argentina, 2003.

Moreno, Hernández Moisés, "Función e importancia de la Política criminal", en *Revista de Política Criminal y Ciencias Penales,* Cepolcrim, agosto, núm. Especial 1, México, 1999.

Vidaurri, Aréchiga Manuel, Bases generales de criminología y política criminal, 1ª Edición, Oxford University Press México, México, 2017.

Fuentes Electrónicas

Cámara de Diputados del H. Congreso de la Unión, Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, http://www.diputados.gob.mx/LeyesBiblio/ref/lgamvlv.htm, fecha de consulta: 25 de septiembre de 2020

Grupo Radioformula, 2020 https://www.radioformula.com.mx/noticias/20190809/diputada-propone-castigar-uso-de-lords-y-ladies-y-la-bautizan-como-ladycensura/ fecha de consulta 17 de agosto 2020

Instituto Nacional de Estadística, Geografía e Informática, 2020 https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2020/EAP_Internet20.pdf fecha de consulta 10 de agosto 2020

S/A, "Presentarán Ley Antimemes", del periódico *EL UNIVERSAL*, 2020, https://www.eluniversal.com.mx/nacion/diputada-del-pes-presentara-ley-antimemes-castigara-modificaciones-en-redes-sociales fecha de consulta 12 de agosto 2020.

Revista Forbes, 2020https://www.forbes.com.mx/las-benditas-redes-sociales-que-le-dieron-like-a-amlo/ fecha de consulta 11 de agosto 2020

Secretaria de Gobernación, 2020, https://www.gob.mx/conavim/articulos/has-sufrido-acoso-cibernetico-te-decimos-a-donde-acudir fecha de consulta 11 de agosto 2020

Secretaria de Seguridad Pública, 2020, http://data.ssp.cdmx.gob.mx/ciberdelincuencia.html fecha de consulta 15 de agosto 2020.

Statista, 2020 https://es.statista.com/estadisticas/1035031/mexico-porcentaje-de-usuarios-por-red-social/ fecha de consulta 19 de agosto 2020

LA IDENTIDAD DIGITAL COMO GARANTÍA CONSTITUCIONAL Y UN MEDIO PARA LA PREVENCIÓN DEL DELITO

David Alejandro Parada Sánchez*
Ingrid Haide Díaz León**

SUMARIO: I. Introducción. II. Los Derechos de la personalidad. III. La extensión del Derecho a la Personalidad y sus garantías. IV. La Identidad Digital. V. La Firma Electrónica. VI. La obligación del Estado de garantizar la Identidad Digital. VII. La Identidad Digital para prevención del Delito. VIII. Conclusiones. IX. Bibliografía.

I. INTRODUCCIÓN

Los avances tecnológicos se han permeado en todos los ámbitos de la vida del ser humano. No hay manera de hablar de la vida humana sin vincularla con algún medio tecnológico. Esto ha traído un cambio sustancial, al grado de determinar el estilo de vida de las personas. Ha pasado de ser una herramienta de auxilio, a ser un medio necesario para entender la realidad. Al grado, que un ser humano que no tenga acceso a las tecnologías, prácticamente se le excluye de la dinámica social.

Al expresar que la tecnología ha definido el estilo de vida, nos referimos en el sentido más amplio de la expresión. Por un lado, se ha hecho más fácil acceder a la información y al conocimiento, maximizar recursos en todos los ámbitos sociales; pero, por otro lado, ha dado lugar a que surjan nuevas formas de cometer ilícitos.

---

* Maestro en Derecho por la Universidad Nacional Autónoma de México, catedrático en la Facultad de Estudios Superiores Acatlán; socio fundador de la firma legal Parius & Parley.

**Egresada de la Carrera de Derecho, UNAM FES Acatlán, Estudiante de la Especialidad de Derecho Fiscal, en el Programa de Posgrado de Derecho, UNAM.

En razón de ello, el Estado se encuentra en una maratónica competencia en la prevención y persecución del delito, pues mientras más avances tecnológicos aplique los grupos delictivos, más medidas debe adoptar el Estado, debiendo llevar la delantera; sin embargo, en no pocas ocasiones, esa aspiración no se alcanza.

El Derecho como Filosofía y Ciencia se ha encargado de observar cada fenómeno social, con el objeto de proponer las normas necesarias para proteger sus Principios, los Derechos Humanos y el Orden Jurídico Constitucional e Internacional. Sin embargo, el desarrollo tecnológico ha sido tan veloz, que es difícil para el legislador emitir paralelamente las disposiciones necesarias para regular cada una de las aplicaciones tecnológicas en el ámbito de vida de las personas; y la emitidas, no siempre son las más idóneas.

El Estado Mexicano ha adoptado mecanismos para incorporar el uso de tecnologías en su actividad, tanto en su organización interna, como para la prestación de servicios públicos. Además, éstos le han facilitado el cumplimiento de sus cometidos y a la ciudadanía el acceso a los mismos, como lo es la Recaudación de Impuestos, la Impartición de Justicia, trámites administrativos en los tres órdenes de gobiernos, incluso la investigación del delito, por solo enumerar unas cuantas. Y con todo ello, se ha ido integrando una Identidad Digital.

La implementación de las tecnologías está generando un alto grado de incertidumbre para quienes acceden a los servicios del Estado por ese medio; también, está ocasionando un enorme rezago y discriminación para acceder a los mismos, excluyendo a los sectores más vulnerables; y con ello, se pierde una gran oportunidad de normalizar los actos públicos y privados para brindar mayor certeza jurídica y prevenir actos contrarios a derecho.

En este artículo, se estudiará y analizará la existencia de la Identidad Digital, se determinará la obligación del Estado de regular la Identidad Digital para garantizar el Derecho a la Personalidad, con

lo cual, se facilitará el acceso a la tecnología y a su vez, el Estado podrá contar con herramientas para prevenir la comisión de delitos.

II. LOS DERECHOS DE LA PERSONALIDAD

Todo ser humano, desde el momento de su nacimiento surge su derecho a la personalidad y a la identidad, por lo que se le reconocen una serie de derechos jurídicos que lo definen como persona. Todos esos atributos en su conjunto harán que la persona, jurídicamente se considera única y diferente a los demás. Permitirán identificarla y vincularla tanto con el Estado, como con la Sociedad a la que pertenece además de permitirle ejercer sus derechos fundamentales dentro de un orden social y jurídico. Ferrajoli expone que, estos derechos corresponden a todos y de éste se derivan derechos primarios de las personas y conciernen indistintamente a todos los seres humanos. Y los derechos públicos, que son los derechos reconocidos a los ciudadanos (Cfr.)[1].

En los Derechos de Personalidad, ubicaremos el derecho a la personalidad, en sentido estricto, a través del cual, el Estado adjudica a cada persona en particular; es un reconocimiento jurídico para adquirir y ejercer derechos públicos y privados. Castán y Castro considera que los derechos de la personalidad pueden entenderse como facultad "de actuar por parte del sujeto que tiene derecho a que se le reconozcan los instrumentos jurídicos necesarios para poder preservar sus bienes y atributos esenciales, que son el contenido propio de los derechos de la personalidad".[2]

Dentro de los derechos de la personalidad, también podemos ubicar el Derecho a la Identidad, pues este Derecho Fundamental le otorga una individualidad jurídica a la persona, diferenciándola

---

1 Ferrajoli, Luigi, Los fundamentos de los derechos fundamentales, 4ª ed., tr. Antonio de Cabo y Gerardo Pisarello, España, Trotta, 2009.Galindo Camacho, Miguel, Derecho Administrativo, México, Porrúa, 1995, p. 23.

2 Castro y Bravo, Federico de, *Apuntes de derecho civil español, común y foral, parte general*, 2ª. ed., Madrid, s.a., p. 268.

de las demás personas. De este modo, todos los derechos que ejerce y obligaciones que adquiere se vinculan a ésta, resultando inconfundible con las esferas jurídicas de las demás personas.

Rosa María Álvarez, explica que "la protección jurídica del derecho a la identidad personal, en su calidad de derecho humano esencial, debe ser integral, para comprender los múltiples y complejos aspectos de la personalidad de un ser humano. La identidad personal hace a la personalidad, como la libertad y la vida."[3]

El contenido del Derecho a la identidad se conforma por el nombre, la nacionalidad, la filiación; y el derecho a la personalidad, se integrará por el Patrimonio y la Capacidad. Es por ello, que en su interdependencia ambos derechos se encuentran estrechamente vinculados y su indivisibilidad resulta evidente, al punto que podría afirmarse que el Derecho a la Identidad es parte del contenido del Derecho a la Personalidad, al formar ambos, parte del contenido de los Derechos de la Personalidad.

En el artículo 6, de la Declaración Universal de los Derechos Humanos, se prevé el derecho la personalidad, señalando: "Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica". Que se reitera en los mismos términos en el artículo 3° de la Convención Americana sobre Derechos Humanos y 16 del Pacto Internacional de Derechos Civiles y Políticos.

Por otro lado, en la Convención sobre los Derechos del Niño, en sus artículos 7 y 8, se establecen el Derecho a la Identidad, al establecer el derecho al nombre inmediatamente después del nacimiento, a adquirir una nacionalidad. Derechos que están expresamente reconocidos en nuestra Constitución en el artículo 29, segundo párrafo, aunque a manera de prohibición, al señalar:

> En los decretos que se expidan, no podrá restringirse ni suspenderse el ejercicio de los derechos a la no discriminación, al reconocimien-

---

3 Álvarez Rosa, María, *Derecho a la Identidad*, Temas selectos de vulnerabilidad y violencia contra niños, niñas y adolescentes. México, UNAM, Instituto de Investigaciones Jurídicas, 2016, p. 116.

> to de la personalidad jurídica, a la vida, a la integridad personal, a la protección a la familia, al nombre, a la nacionalidad; los derechos de la niñez; los derechos políticos; las libertades de pensamiento, conciencia y de profesar creencia religiosa alguna; el principio de legalidad y retroactividad; la prohibición de la pena de muerte; la prohibición de la esclavitud y la servidumbre; la prohibición de la desaparición forzada y la tortura; ni las garantías judiciales indispensables para la protección de tales derechos.

Podría generar un debate si el derecho a la personalidad y a la identidad, son derechos fundamentales diversos; o el segundo, forma parte del primero. A fin de no entrar en este debate, del cual seguramente hay mucho que analizar, para efectos de esta investigación, nos referiremos como Derecho a la Personalidad, considerando como parte de este el Derecho a la Identidad, ello en atención a que civilmente se considera como atributos de la personalidad, el nombre y la nacionalidad; y también, porque el Derecho a la Personalidad tiene un mayor alcance que su homólogo.

Como derecho fundamental, el Estado Mexicano está obligado a garantizar su protección, de conformidad con el artículo 1° Constitucional, y como bien lo ha sostenido, más aún al tratarse de un derecho a favor de la libertad, para con ello configurar el ideal de bien común que "consiste precisamente en posibilitar la autodeterminación individual"[4]

En esta obligación del Estado de garantizar los Derechos Fundamentales deberá hacerlo a través de medios idóneos y razonables que permitan jurídica y materialmente un auténtico ejercicio de los mismos. De no hacerlo, incurriría en una vulneración al derecho fundamental, que se puede configurar por un hacer o un no hacer. En el caso del Derecho a la Personalidad, el Estado tiene una obligación mixta, la cual analizaremos más adelante.

---

4 Grimm Dieter, *Constitucionalismo y Derechos Fundamentales,* Madrid, Trotta, 1ª ed, 2006, p.79

III. LA EXTENSIÓN DEL DERECHO A LA PERSONALIDAD Y SUS GARANTÍAS

Siguiendo la clasificación de Ferrajoli, las garantías pueden ser negativas o positivas, lo cual será correspondiente al Derecho Fundamental que se pretenda proteger, respetar o reparar. Así, las primeras implican una conducta de no hacer o abstención para el Estado y la segundas un hacer para el Estado:

> Los derechos fundamentales, de la misma manera que los demás derechos, consistente en expectativas negativas o positivas a las que les corresponden obligaciones (de prestación) o prohibiciones (de lesión). Convengo en llamar garantías primarias a estas obligaciones y a estas prohibiciones, y garantías secundarias a las obligaciones de reparar o sancionar judicialmente las lesiones de los derechos, es decir, las violaciones a las garantías primarias.[5]

En el caso del Derecho a Identidad como parte del Derecho a la Personalidad, al Estado le corresponde en un inicio un hacer, esto es, debe establecer las normas que jurídica y materialmente lo protejan y garanticen. Así, el derecho a la personalidad se garantiza al reconocer su contenido:

Derecho al nombre. Se integra por el nombre de pila y los apellidos que lo acompañan. La Primera Sala de la Suprema Corte de Justicia de la Nación, explica que el derecho humano tiene la finalidad de fijar la identidad de una persona en las relaciones sociales y ante el Estado, que le da individualidad al sujeto, al ser un signo distintivo del individuo ante los demás; es inalienable e imprescriptible (Cfr.).[6]

---

5 *Op. Cit.*, p. 27.

6 Tesis 1a. XXXII/2012 (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro VI, Marzo de 2012, Tomo 1, p. 275.

Derecho a la nacionalidad. Es el vínculo jurídico que existe entre una persona y un Estado, adquirido por nacimiento o por un acto jurídico posterior. La Organización de las Naciones Unidas, explica que el derecho a la nacionalidad es un derecho humano fundamental, que comprende el derecho de cada persona a adquirir, cambiar o retener una nacionalidad, en tanto, los Estados deben cumplir con sus obligaciones de derechos humanos en lo tocante a la concesión o la retirada de la nacionalidad.[7]

Derecho a la identidad. "Es la necesidad y la capacidad que tiene un individuo de encontrar lazos psicológicos, sociales, culturales, y grupos humanos como la familia, una sociedad y una nación en general. De igual forma, constituye la capacidad de encontrar su propio lugar en todos los aspectos mencionado en sí mismo, e involucrarlos en su desarrollo personal."[8]

La capacidad jurídica. Se trata de la cualidad del individuo para ser sujeto de derechos y obligaciones, así como, ejercer derechos directamente; así como, adquirir y cumplir obligaciones con efectos jurídicos plenos ante el Estado y terceros.

IV. LA IDENTIDAD DIGITAL

Los avances tecnológicos han dado a las personas diversos espacios de expresión no físicos, pero que influyen en la construcción social de la persona, como lo son: las redes sociales, aplicaciones de mensajería, correo electrónico y hasta las video llamadas; a través de los cuales se extiende la vida social. A esto se le denomina Identidad Virtual:

> Se pueden establecer paralelismos entre la vida real y la virtual que conllevan a patrones comunes de identidad en el in-

---

7 Oficina del Alto Comisionado de las Naciones Unidas, *Derecho a la nacionalidad y apatridia,* artículo cosnultado el 19 de agosto de 2020, en https://www.ohchr.org/SP/Issues/Pages/Nationality.aspx

8 *Op. Cit*, Álvarez Rosa María, p. 117.

> dividuo. La identidad virtual es fluida; se basará, al igual que la social, en ajustes provocados por la naturaleza de las circunstancias. La fluidez de la identidad, así como de nuestra sociedad (sobre la cual hablaban Bauman o Beck), es una vía de adaptación al mundo.
>
> Resumiendo, en la identidad virtual confluyen tanto fenómenos de identidad colectiva (que me asemejan o alejan del grupo) como individual o personal (identificándonos con diferentes identidades). Pero el estudio de la identidad virtual precisa del análisis de otros componentes tales como nuestros comportamientos en la red así como el entendimiento del cuerpo virtual como parte esencial de nuestra identidad.[9]

Por otro lado, el propio avance tecnológico ha permitido que las personas estén en posibilidad de realizar actos jurídicos válidos a través del internet, tanto públicos como privados. La persona contrae y cumple obligaciones, así mismo, ejerce derechos exigibles por el Estado y por terceros, configurando así la Identidad Digital de la persona.

La identidad virtual tiende a un concepto sociológico y no debe confundirse con la Identidad Digital, puesto que la primera tiende a la integración del individuo en una sociedad que se desenvuelve a través de los diversos espacios en internet, lo que le permite al sujeto ir construyéndose una propiedad identidad, o varias, a través de Blogs, Microblogs, Sitios Web, Redes Sociales y cualquier otro medio de comunicación con las demás personas. En cambio, la Identidad Digital se va integrando de todos las acciones y omisiones realizadas en un entorno digital, con eficacia jurídica y que se vinculan a una persona, como lo es, la celebración de un contrato, la promoción de un juicio, la declaración de impuestos, por mencionar algunos ejemplos.

---

9 Muros, Beatriz, *El concepto de identidad en el mundo virtual: el yo online.* España, Revista Electrónica Interuniversitaria de Formación del Profesorado, *vol. 14, núm. 2*, Asociación Universitaria de Formación del Profesorado, pp.51 y 52

La Identidad Digital se va construyendo en el ciberespacio por el propio sujeto y sus efectos o consecuencias se establecen en la propia norma o regulación aplicable. En cambio, en el Yo virtual, no debería generar obligaciones jurídicamente exigibles, aunque accidentalmente lo puede hacer al celebrar actos jurídicos a través de algún canal de comunicación electrónico, como las redes sociales o servicios de mensajería. Sin embargo, ello no produciría efectos en la Identidad Digital, pues la obligación que surgió en el Yo virtual, derivaría de una ficción de celebración de actos entre no presentes, generando incertidumbre sobre la validez del acto, incluso sobre la identidad de la persona.

La Identidad Digital permite que el Estado vincule al sujeto a actos y negocios jurídicos, que forman parte de la esfera jurídica de la persona. Brinda una certeza jurídica respecto de los actos celebrados y realizados bajo la identidad digital. Contrario a la Identidad Virtual, en la cual, se podrían crear usuarios ficticios, en la Identidad Digital se individualiza a la persona, atribuyéndole de manera certera la realización y celebración de actos de índole pública y privada.

A través de la Identidad Digital, la persona puede ejercer diversos derechos fundamentales como lo es la libertad económica para celebrar contratos o convenios civiles o mercantiles; derecho de acceso a la justicia al poder promover juicios; derecho a la Buena Administración Pública al realizar trámites ante autoridades administrativas; al igual, cumplir con obligaciones como lo son las fiscales.

En este sentido, resulta necesario que el Estado garantice la Identidad Digital, estableciendo medios y mecanismos sencillos que le permitan al sujeto realizar actos y negocios jurídicos que le brinden total certeza y se incorporen válidamente dentro de su esfera jurídica. A su vez, debe proteger y garantizar el ejercicio de esta, al crear normas que brinden protección de datos personales, privacidad, seguridad y disponibilidad:

> La identidad digital permite el reconocimiento y actuación de los individuos, las corporaciones o los poderes públicos en Internet. La ciberseguridad tradicional se ocupa de proteger la confidencialidad, integridad y disponibilidad de los sistemas, las redes y la información que discurren por Internet, pero la eclosión de la digitalización exige, además, salvaguardar los derechos y la reputación de quienes utilizan la identidad digital.
>
> La protección de la identidad digital (online) se desarrolla, por un lado, asociando la protección de derechos como la privacidad, el olvido o el anonimato a la de otros derechos fundamentales mediante la regulación y la jurisprudencia y, por otro, desarrollando mecanismos de identificación y autenticación que proporcionen un uso seguro de Internet y el aprovechamiento de las posibilidades y nuevos modelos de negocio que ofrece la economía digital.[10]

Por sus características, la Identidad Virtual es una manifestación del Derecho a la Libertad, lo que vincula al Estado para una obligación de no hacer, es decir, con el solo hecho de no intervenir en ésta, el Estado respeta la Libertad de la persona. En cambio, la Identidad Digital requiere por parte del Estado una serie de acciones para respetarlo y protegerlo, puesto que el sujeto requiere que se le proporcionen herramientas necesarias para poder ejercerlo; de no ser así, no contaría con medios para brindar certeza jurídica en la celebración de sus negocios privados, o bien, promover juicios por medio de la red.

Por lo que resulta necesario, que se considere a la Identidad Digital como parte del contenido del Derecho a la Personalidad (incluso del Libre Desarrollo de la Personalidad), con el objeto de que el Estado se vea obligado a garantizar el ejercicio de este derecho y a protegerlo, sobre todo, en sus parámetros de ejercicio como lo es

---

10 Alonso Lecuit, Javier, *Identidad Digital y seguridad online, Ciber Elcano número 53, Elcano Royal Institute, España, consultado el 20 de agosto de 2020, en http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciber-elcano-53-marzo-2020*

la privacidad, el anonimato y la identidad auto soberana, es decir, una identidad digital universal.

A su vez, se le brindaría total seguridad jurídica y protección a los Derechos Fundamentales de terceros, puesto que sería un mecanismo para tener plena certeza de la identidad de la persona y darle validez a los actos jurídicos que llegare a celebrar.

En España se cuenta con un mecanismo a través del cual se pretende garantizar la Identidad Digital, esto es, el documento denominado Documento Nacional de Identidad Electrónico, que emite la Dirección General de la Policía, el cual permite:

- Acreditar electrónicamente y de forma inequívoca la identidad de la persona.
- Firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita[11]

Con este documento se asigna una firma electrónica y un certificado digital, con el cual, se garantiza el ejercicio de la Identidad Digital, al permitirle a la persona realizar de forma segura, cualquier tipo de acto y negocio jurídico con autoridades administrativas, empresas públicas y privadas y con otros particulares.

Es necesario mencionar, que en México a pesar de que se ha impulsado el uso de la firma electrónica, ello no garantiza el Derecho a la Identidad Digital, porque no es uniforme y se ha creado con la finalidad de cumplir con una formalidad para facilitar algunos trámites normativos y no bajo la lógica de garantizar un derecho fundamental. Lo cual será materia de análisis en el siguiente tema.

V. LA FIRMA ELECTRÓNICA

Hace un par de años, para realizar trámites o interponer juicios ante dependencias públicas, así como celebrar contratos públicos y priva-

11 Portal "Usa tu DNI", consultado en http://www.usatudni.es/

dos solo era posible mediante la firma autógrafa de la persona en los documentos que esta exhibía, con el fin de autentificar su identidad.

Con el paso del tiempo y derivado de las circunstancias que atraviesa el país en la actualidad (este artículo se escribe durante la Pandemia por COVID-19), se ha impulsado con mayor énfasis la necesidad de implementar mecanismos para disminuir las actividades presenciales de las personas, lo que llevó a la necesidad de implementar mecanismos tecnológicos que permitan autentificar la identidad de la persona.

Desde el 11 de enero de 2012 inició vigencia la Ley de la Firma Electrónica Avanzada, con la cual se reguló la aplicación y uso de la firma electrónica en los actos, procedimientos y trámites que se llevan a cabo en las dependencias, entidades o cualquier órgano, así como los actos llevados a cabo ente particulares. Con ésta otorga el mismo valor jurídico que tiene la firma autógrafa a la firma electrónica, regulando además el proceso de certificación de la misma, no obstante, ello no ha sido suficiente para garantizar el Derechos a una Identidad Digital.

En el artículo 2°, fracción XIII, de la Ley de la Firma Electrónica Avanzada, La Firma Electrónica se define como el "conjunto de caracteres que permiten la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos de la firma autógrafa." Con esta definición, no hay duda alguna que la Firma Electrónica es un mecanismo vinculado a la Identidad Digital.

A su vez esta ley establece los requisitos para el uso de esta firma los cuales son:

- **Equivalencia funcional**: La firma electrónica avanzada tiene el mismo valor que la firma autógrafa.
- **Autenticidad**: Da certeza de que la firma ha sido emitida por el firmante, por lo que su contenido y las consecuencias

que de esta deriven son atribuibles a la persona que firma.

- **Integridad**: Da certeza de que el documento que contenga la firma electrónica está completo e inalterado desde su firma, con independencia de los cambios que hubiere podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación.
- **Neutralidad Tecnológica**: La tecnología utilizada para la emisión de los certificados digitales y para la prestación de servicios relacionados con la firma será aplicada de tal modo que no excluya, restrinja o favorezca alguna tecnología en particular.
- **No repudio**: Garantiza la autoría e integridad del documento, así como que dicha firma corresponde al firmante.
- **Confidencialidad**: Garantiza que solo puede ser cifrado por el firmante y el receptor.

Para dar certeza de la Identidad de la persona, la firma electrónica debe contar con un certificado digital vigente emitido u homologado por la autoridad certificadora como lo es la Secretaría de la Función Pública, la Secretaría de Economía y el Servicio de Administración Tributaria; además de una clave privada que genere el firmante; teniendo la obligación de comprobar la veracidad de los datos y documentos que proporcionó para su identificación personal.

Hoy en día, se busca crear formas que nos permitan realizar fácil y rápido actividades como lo son trámites ante dependencias públicas, juicios y actos celebrados entre particulares; de aquí es que surge la necesidad de que el Estado como un ente que salvaguarda los derechos de sus ciudadanos amplié a través del uso de tecnologías uno de los derechos más importantes que poseemos que es el derecho a la identidad y lo optimice hacia la Identidad Digital.

Partiendo de que los derechos humanos son progresivos, debe buscarse en todo momento ampliarlos y adecuarlos a los tiempos actuales; en el caso del derecho a la identidad, es evidente el hecho

de que una identidad plasmada en papel ya no es suficiente, por lo que haciendo uso de la tecnología se llega a una materialización de esta que es la "Identidad Digital", la cual, va más acorde con los tiempos actuales(Cfr.).[12]

La validez legal de estas actividades radica en el consentimiento que da la persona que las realiza a través de su firma, la cual con el paso del tiempo ha ido modernizándose hasta llegar a lo que hoy conocemos como firma electrónica avanzada. Esta transición de lo material a lo digital ha sido un gran reto para las instituciones como el Servicio de Administración Tributaria y el Poder Judicial de la Federación, las cuales han implementado cada una su propia firma electrónica para facilitarle a los ciudadanos el acceso a los servicios que estas ofrecen(Cfr.).[13]

La firma electrónica llegó para sustituir paulatinamente lo que conocemos como firma autógrafa, trayendo consigo ventajas como el poder autentificar un documento, identificando fácilmente al autor de este, garantizando la integridad del mismo. También significa una reducción considerable en el uso de papel para la elaboración de documentos, permitiendo organizar mejor los documentos electrónicos en la nube o en algún dispositivo de almacenamiento en lugar de archivarlos físicamente. Da certeza en los documentos porque una vez firmados con la firma electrónica avanzada no pueden ser modificados o alterados.

A su vez, en el caso de personas que se dedican a la actividad empresarial, el uso de la firma le ofrece a la persona una mejora significativa en el desarrollo de sus actividades, agilizando el trato con sus clientes en el caso de la venta de productos o servicios; como ejemplo de esto tenemos el caso de los bancos que permiten el uso de la firma digital para realizar procedimientos, transacciones o

---

12 "Vázquez Cruz Edgar. "Identidad Digital: Una tarea inaplazable para el Estado Mexicano" de la Revista *Mundo Contact*, 8 de Julio de 2015.

13 García Inclan, Raquel Margarita, "La Firma Electrónica desde un Punto de Vista Jurídico", México, Editorial Porrúa, 1ª ed., p. 67.

aclaraciones de forma digital, brindándole así seguridad a sus clientes respecto de las operaciones que realizan.

Derivado de la pandemia de COVID-19 que se vive a nivel mundial y que ha tenido repercusiones políticas, sociales y económicas para todos los países del mundo, el uso de tecnologías para realizar trámites ante instituciones públicas, tener acceso a la justicia en Juzgados y tribunales a través de los juicios en línea, realizar actividades entre particulares como la celebración de contratos; actividades que apenas empezaban a implementarse a modo de "sistema piloto", se han vuelto una tarea inaplazable para las personas en la actualidad, lo cual nos ha obligado a pasar de una transición lenta del uso de tecnología a un rápido intento de adaptación.

En el caso de México, el uso de la firma electrónica avanzada (la e.firma que es proporcionada por el Servicio de Administración Tributaria-SAT) se ha ampliado no solo para realizar trámites ante SAT, sino además se está implementando para presentar demandas, recursos y promociones ante Tribunales, así como para acceder a los expedientes electrónicos en el caso de las personas que no cuentan con la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL), ya que la Segunda Sala de la Suprema Corte de Justicia de la Nación determinó que es válido presentar demandas de amparo con firma electrónica, en razón de existe convenio de coordinación con el Poder Judicial de la Federación para el reconocimiento de los certificados digitales homologados emitidos por otros órganos del Estado como lo es el SAT.[14]

Lo que se busca es que las personas puedan realizar este tipo de actividades sin tener que salir de sus casas, evitando así aglomeraciones de personas esperando ingresar documentos físicos en las diferentes dependencias que permiten el uso de esta firma, al darle el mismo valor de una firma autógrafa.

---

14 Contradicción de tesis 220/2017, Semanario Judicial de la Federación del viernes 27 de febrero de 2015 a las 9:30 horas y en la Gaceta del Semanario Judicial de la Federación, Décima Época, Libro 15, Tomo III, febrero de 2015, página 2669.

De primera instancia, esto podría verse como un gran avance tecnológico para el país, el cual le permite a las personas realizar de forma rápida y segura estas actividades; pero esta tecnología no garantiza no protege el Derecho a la Identidad Digital.

Sin embargo, incumple con la característica de Privacidad y Anonimidad, porque al utilizar una firma electrónica expedida por una autoridad fiscal para promover juicios, le da conocimiento a la autoridad fiscalizadora de actos que no son de su competencia, teniendo conocimiento de litigios que podrían implicar hasta datos sensibles; además del riesgo que pueda ser utilizada como una medida recaudatoria, porque se podría fiscalizar el monto económico que implique cada juicio.

Por otra parte, en cuanto a la celebración de contratos entre particulares, también es una transgresión de la privacidad de la persona que celebre un contrato de cualquier índole, mediante la e.firma el SAT, pues ésta tendría conocimiento de la celebración de contratos, es decir, intervendría en asuntos de índole totalmente privada.

Si bien, puede considerarse como ventaja el hecho de poder firmar un contrato en cualquier parte utilizando la firma electrónica y teniendo la confianza de que con esta, la identidad de los celebrantes queda totalmente autentificada y este ya no puede ser modificado; también debe reconocerse que el ampliar el uso que se le da a la e.firma para actos que no son realizados ante el SAT, implica el permitirle a esta autoridad que esté enterada de todos los actos que realiza la persona, violentando su privacidad.

La implementación y uso extendido que se le está dando a la firma electrónica emitida por el SAT, por sí misma violenta el Derecho a la Identidad, pues no es una autoridad competente para que su firma tengan validez en actos jurídicos fuera de su competencia. Esto es, no debería tener validez para firmar demandas o promociones en juicos de naturaleza familiar como un divorcio, pensión alimenticia o algún tema penal, civil o mercantil por mencionar algunos ejemplos. Puesto que se trata de actos públicos que nada

tienen que ver con la materia fiscal, pero que el SAT puede utilizar para para realizar actos de fiscalización.

Por otro lado, los propios Tribunales han dado como opción el uso de una firma electrónica administrada por éstos mismos, sin embargo, ello ha llevado a los ciudadanos a contar con tantas firmas electrónicas como instituciones las requieran, por enunciar algunas, tenemos al SAT, el Poder Judicial Federal, el Tribunal Superior de Justicia del Estado de México; además de las empresas privadas que expiden sus propias firmas electrónicas.

Esto ha llevado a los ciudadanos a encontrarse con un gran obstáculo y confusión para obtener sus diversas firmas electrónicas. Por ello, resulta claro que los usos actuales de las firmas electrónicas en México no respetan ni garantizan el Derecho a la Identidad Digital.

Es un hecho que una firma electrónica universal garantizará el Derecho a la Identidad Digital, y se debe garantizar que su uso no implique una afectación a nuestros derechos humanos como lo es nuestra privacidad; debiendo aclarar que esta firma por sí misma, no debe excluir la posibilidad de que cada institución cuente con su propia firma electrónica, si así lo adoptan, pero la firma electrónica universal también debería ser reconocida.

VI. LA OBLIGACIÓN DEL ESTADO DE GARANTIZAR LA IDENTIDAD DIGITAL

El Estado está obligado a reconocer aquellos derechos que se consideran necesarios y esenciales para proteger el Derecho a la Vida, la Libertad, la Igualdad y la Dignidad, a fin de que sean considerados Derechos Fundamentales. De ese modo, surge su obligación de crear los mecanismos normativos y fácticos para que el Derecho Fundamental pueda ejercerse con efectividad.

Es importante destacar que no necesariamente se requiere una reforma constitucional, pero sí un reconocimiento por parte del Legislativo en norma secundaria o una interpretación por parte de los

Tribunales Federales para que este Derecho se considere parte del contenido del Derecho a la Personalidad y con ello, sería exigible por los Ciudadanos que se garantice.

La Identidad Digital era un derecho impensable hace un par de décadas, sin embargo, la modernidad y actualidad exigen del Estado su reconocimiento a fin de cumplir con la optimización del Derecho Fundamental.[15] Alexy considera que la protección de los Derechos Fundamentales deberá realizarse en la medida de lo posible, es decir, que queda condicionado a lo materialmente y jurídicamente factible (Cfr.).[16]

Para el Estado Mexicano no existe impedimento alguno para reconocer y garantizar este Derecho. Incluso el uso de la firma electrónica por parte de las autoridades administrativas y judiciales, como se analizó previamente, es un perfecto ejemplo de que se cuenta con la capacidad material, económica y jurídica para poder garantizar este derecho.

No obstante, no es suficiente para afirmar que el Estado Mexicano ya está cumpliendo con su obligación de garantizar la Identidad Digital, porque es necesario homogenizar la firma electrónica y su certificado en uno solo. Para el ciudadano mexicano resulta complejo contar con tres, cuatro o más firmas electrónicas, generando confusión y dificultad en obtenerla; esto a su vez, provoca que los Derechos Fundamentales que se pretendan ejercer con la firma electrónica se vean obstaculizados.

A manera de ejemplo, una persona que tenga la necesidad de promover un Juicio de Amparo y lo pretende hacer en línea, se vería con dificultad de tener que tramitar y obtener la firma electrónica del Poder Judicial Federal, en caso de no contar con la Firma Elec-

---

15 Bernal Pulido, Carlos. El principio de proporcionalidad y los derechos fundamentales: El principio de proporcionalidad como criterio para determinar el contenido de los derechos ... para el Legislador (*Spanish Edition*), versión Kindle, España, 2014, pos 12827.

16 Alexy, Robert, *Teoría de la Argumentación Jurídica*, tr. Manuel Atienza e Isabel Espejo, España, Dentro de Estudios Políticos y Constitucionales, 2ª. ed., 2014, p. 350

trónica que proporciona el Servicio de Administración Tributaria; y de contar con las dos, o más firmas de otras instituciones, tendrá que estar actualizando el certificado digital para cada una de manera periódica para evitar que caduque.

En la optimización de los Derechos Fundamentales, el Estado debe adoptar los medios más adecuados para lograr la Mayor Protección al Derecho Fundamental, en este caso, el medio más idóneo para garantizar la Identidad Digital, es la expedición universal de una firma electrónica única para cada ciudadano mexicano que obtenga la mayoría de edad, con reconocimiento y uso en todos los ámbitos público y privado, y en los tres órdenes de gobierno.

De este modo, se facilitaría la construcción e integración de la Identidad Digital, puesto que la persona podría utilizar la firma electrónica universal para cualquier trámite administrativo, judicial, incluso privado para efectos del comercio electrónico, respecto el cual, cabe mencionar que no se ha logrado su consolidación, justamente por la dificultad de contar con una firma electrónica.

Es relevante precisar que esta firma debe ser administrada por un organismo constitucionalmente autónomo, que garantice la privacidad de la misma y su anonimato ante terceros, pero que brinde seguridad en su uso. Por lo que se considera, que debe ser Instituto Nacional Electoral el competente para ello, al ser la autoridad que expide la credencial de elector de la persona, es decir, es un órgano que se vincula con el Derecho a la Personalidad al expedir el documento que le da identidad a un ciudadano, al menos en lo que se refiere a su nombre y nacionalidad.

VII. LA IDENTIDAD DIGITAL PARA PREVENCIÓN DEL DELITO

Garantizar la Identidad Digital, no solo implica una ventaja para las personas, sino que también genera un medio adecuado para la Prevención del Delito, porque al darle a cada persona una identidad

única dentro del ciberespacio, permitirá brindar certeza jurídica sobre los actos que realiza, logrando prevenir delitos como el lavado de dinero, evasión fiscal, defraudación, simulación de actos jurídicos que podría llevar a estafas, robo o suplantación de identidad.

Se considera así, porque l podría establecerse que toda operación comercial vía internet, las personas deban identificarse digitalmente, para tener total certeza de su identidad. En el caso de lavado de dinero facilitaría el seguimiento de los recursos, desde su incorporación al sistema financiero hasta su salida.

Al ordenarse que todas las transacciones a partir de cierto monto deban ser validadas con la Identidad Digital, se evitará que seas realizadas operaciones comerciales usurpando la identidad de otras personas, pues al tener que validar la firma electrónica, se limitará sustancialmente esas prácticas.

Desde el punto de vista de los delitos fiscales, le permitirá a la autoridad hacendaria, dar seguimiento del monto de las operaciones realizadas, y así, no depender únicamente de las operaciones registradas en instituciones financieras; para lo cual, debemos considerar que en la red es posible realizar transacciones económicas a través de otros servicios, no regulados y de difícil control, como ocurre con las recientes Instituciones de Tecnología Financiera, el Trading con Criptomonedas o las plataforma con esquemas novedosos de inversión.

Con la implementación de la Identidad Digital, cada persona tendrá la alternativa de poder exigir en las plataformas digitales que, se puedan celebrar sus transacciones con el uso de la firma electrónica, para dar mayor seguridad a sus operaciones y, así disminuir el riesgo de que puedan ser víctimas de un delito de fraude.

Proyectando la Identidad Digital hacia el futuro, podría establecer las condiciones para que, de manera voluntaria, cada persona se autentifique en redes sociales, mensajería o cualquier otro servicio tecnológico; a fin de que su imagen pueda ser sujeta a mayor protección y evitar que su identidad sea usurpada. Claramente esto

hará que surjan nuevas conductas que el Estado deberá prevenir, como lo es el robo de la firma electrónica, el hackeo de la Identidad Digital de la persona, pero son costos necesarios para garantizar este derecho.

El ciberespacio es enorme y los avances tecnológicos tan acelerados, que resulta complicado para el Estado, los investigadores, juristas y legisladores prever todas las nuevas situaciones que surjan ante el avance tecnológico. Por ello, deben preverse medios adecuados que puedan moldearse sin que dependa únicamente de la emisión de disposiciones normativas. Y se considera que una adecuada regulación de la Identidad Digital, permitirá ese ajuste paralelo, pues las propias personas tendrán la posibilidad de decidir si realizan algún acto jurídico con el uso de su firma electrónica universal, para disminuir la posibilidad de que sea víctima de un delito o no hacerlo.

VIII. CONCLUSIONES

El Derecho a la Personalidad implica la necesidad de cada persona de ser identificada como única, que le permita ser reconocida dentro de la sociedad y por el Estado, con la finalidad de que esté en posibilidades de ejercer sus derechos, contraer y cumplir con sus obligaciones, así como, exigir ante el Estado el cumplimiento y respeto de sus derechos públicos, privados y fundamentales.

El desarrollo tecnológico ha creado nuevos espacios de desenvolvimiento y convivencia de la persona, en la que incluso puede crearse una personalidad totalmente distinta a la reconocida socialmente, surgiendo así la identidad virtual. Por otro lado, en el mismo ciberespacio la persona se va construyendo una personalidad necesaria para realizar actos jurídicos ante las autoridades y negocios jurídicos con particulares, con plena eficacia jurídica.

En ese escenario, resulta necesario que el Estado reconozca el Derecho a una identidad Digital como parte del Derecho a la Per-

sonalidad, a fin de garantizar a las personas que puedan ser plenamente identificados e individualizados en el ciberespacio. Lo cual les brindará mayor certeza y seguridad jurídica respecto de los actos y negocios que celebren en este ámbito.

Con el reconocimiento y regulación del derecho a la Identidad Digital, se tendrá un medio adecuado para prevenir los delitos y en su caso, contar con mayores herramientas para la investigación de los mismos. Incluso, dará mayor certeza de la identidad de las personas que participaron en su comisión.

Por lo tanto, es imperativo que el Estado Mexicano reconozca el Derecho a la Identidad Digital.

IX. FUENTES CONSULTADAS

Bibliografía

Alonso Lecuit, Javier, Identidad Digital y seguridad online, Ciber Elcano número 53, Elcano Royal Institute, España, consultado el 20 de agosto de 2020, en http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciber-elcano-53-marzo-2020

Alexy, Robert. Tres escritos sobre los derechos fundamentales y la teoría de los principios, tr. Carlos Bernal Pulido, 1ª ed, Universidad Externado de Colombia, Colombia, 2003, edición Kindle, pos. 155.

Álvarez Rosa, María, Derecho a la Identidad, Temas selectos de vulnerabilidad y violencia contra niños, niñas y adolescentes. México, UNAM, Instituto de Investigaciones Jurídicas, 2016.

Bernal Pulido, Carlos. El principio de proporcionalidad y los derechos fundamentales: El principio de proporcionalidad como criterio para determinar el contenido de los derechos ... para el Legislador, 4ª ed., Universidad Externado, Edición de Kindle, Colombia, 2014.

Castro y Bravo, Federico de, Apuntes de derecho civil español, común y foral, parte general, 2a. ed., Madrid, s. a.

Ferrajoli, Luigi, Los fundamentos de los derechos fundamentales, 4ª ed., tr. Antonio de Cabo y Gerardo Pisarello, España, Trotta, 2009.

García Inclan, Raquel Margarita, "La Firma Electrónica desde un Punto de Vista Jurídico", México, Porrúa, 1ª ed., 2007.

Grimm Dieter, Constitucionalismo y Derechos Fundamentales, Madrid, Trotta, 1ª ed, 2006.

Muros, Beatriz, El concepto de identidad en el mundo virtual: el yo online. España, Revista Electrónica Interuniversitaria de Formación del Profesorado, vol. 14, núm. 2, Asociación Universitaria de Formación del Profesorado.

Material Consultado

Oficina del Alto Comisionado de las Naciones Unidas, Derecho a la nacionalidad y apatridia, artículo consultado el 19 de agosto de 2020, en https://www.ohchr.org/SP/Issues/Pages/Nationality.aspx

"Usa tu DNI", España, consultado el 20 de agosto de 2020, en http://www.usatudni.es/

Vázquez Cruz, Edgar Identidad Digital: Una tarea inaplazable para el Estado Mexicano, México, Revista Mundo Contact, 8 de julio de 2015, consultado en https://www.edgarvasquez.com/identidad-digital-tarea-inaplazable/

Semanario Judicial de la Federación, Suprema Corte de Justicia de la Nación, consultado en https://sjf.scjn.gob.mx/sjfsist/paginas/tesis.aspx

REFLEXIONES EN TORNO A LA PREVENCIÓN DEL DELITO DE TRATA DE NIÑAS MENORES DE EDAD A TRAVÉS DE LAS REDES SOCIALES

José Antonio Alvarez León*
Carla María Escoto**

SUMARIO: I. Introducción. II. Nuevo espectro del control del delito. III. Redes Sociales y Medios Tecnológicos en la Comisión de Delitos. IV. Trata de Mujeres Menores de Edad. V. Prevención Tecnológica. VI. Epilogó VII. Fuentes de Consulta.

I. INTRODUCCIÓN

La trata de personas en México es un delito grave y sus cifras van en aumento. Hasta hace algunos años su realización se daba únicamente en el espacio físico aunque sus modalidades siguen siendo muy diversas pues lo mismo se ataca a menores de edad, mujeres mayores, turistas y migrantes. La trata de personas, el secuestro, la violación y el homicidio son delitos donde la dignidad de las personas es mancillada de forma brutal y requieren de su pronta atención; sin embargo, estos hechos delictivos se han multiplicado porque han encontrado en los espacios virtuales un lugar más amplio, para buscar víctimas, esconderse, negociar y articular estrategias dentro y fuera de la red.

Los tratantes de personas, han ido seleccionando de forma exponencial su victimas particularmente menores de edad y con mayor agudeza tratándose de niñas. El uso de las tecnologías de la información les ha facilitado entrar en contacto directo con sus posibles

---

*José Antonio Alvarez León. Profesor investigador en el departamento de Posgrado en Derecho y Política Criminal. Fes Acatlán UNAM.

** Licenciada en Derecho por la FES Acatlán. Aspirante al Posgrado en Derecho.

víctimas mediante la simulación; en muchos casos usando fachadas o disfrazando la personalidad, en otros, usando cómplices jóvenes o simplemente mediante otras formas del engaño.

El problema central está en la gran facilidad que tiene el delincuente para moverse dentro y fuera de la red y articular su actuar con varios sujetos sin siquiera exponerse. Los tipos penales pueden quedar desprovistos del encuadramiento requerido ante la movilidad de ejecución delictiva que hace difícil su investigación y acreditación.

En México, el problema es más grave aún, pues las mismas leyes carecen de conceptos básicos para poder determinar que los medios comisivos como el uso de plataformas virtuales son las formas más comunes para enganchar a sus posibles víctimas y más aún a las señoritas adolescentes y menores de edad.

De esta manera, el objeto del presente ensayo es exponer los elementos básicos del delito de trata de personas particularmente niñas a través de las redes sociales y reflexionar, respecto de la vulnerabilidad de las personas ante la falta de certeza legal y de estrategias tecnológicas preventivas en este tema. Se busca dar cuenta que el combate al delito de trata es cada vez más complejo y se requieren políticas desde los medios tecnológicos y políticas de Estado que alerte a padres y menores de edad ante un tema tan grave como este.

Los delitos cibernéticos básicamente se dan bajo tres premisas, la primera, el desconocimiento serio y responsable del uso del espacio virtual y el medio de interacción; segundo, la sorpresa, factor clave para la comisión de los delitos de forma particular en los cibernéticos porque en la mayoría de los casos lo usuarios son más empíricos que al menos medianamente letrados en su práctica. Tercero, el uso indebido o incorrecto, la mayoría de las personas curiosean en la red buscando y viendo todo tipo de cosas son sin saber que alguien los puede acechar o sorprender o simplemente saber dónde se está y a qué se pueden vincular *(sitio web)*.

En la trata de personas desafortunadamente la búsqueda de mujeres muy jóvenes es un motivo de premura para buenos negocios.

Sorprender a las niñas, robándoles información o vinculándose con ellas mediante el engaño es la estrategia delictiva más común es por eso que este trabajo trata de evidenciar la necesidad disminuir riesgos para ellas mediante estrategias de prevención.

II. NUEVO ESPECTRO DEL CONTROL DEL DELITO.

Uno de los problemas más comunes dentro del campo de la política criminal es sin duda el control del fenómeno delictivo. Como ya se sabe, el delito se caracteriza por ser relativo de un lugar a otro debido a las condiciones que lo generan y por cómo se desarrolla. Esta condición no cambiará y será un efecto determinante para entender su combate y prevención; sin embargo, cada vez se reafirma una nueva característica de ejecución del delito, en la teoría y en la *práxis* y se considera "nueva modalidad delictiva", nos referimos a la fragmentación del delito. Esto significa que en el desarrollo del delito cambiaba el *modus operandi* y el lugar físico, con ello se obligaba a que el legislador incluya una nueva circunstancia típica que retrate dicho móvil, cada que aparece nueva forma de ejecución "El crimen existe, así, como efecto de la construcción social y de la imposición del rotulo de crimen[1]", pues cada que la sociedad avanza el delitos también lo hacen.

Cuando se da una nueva circunstancia típica se ve como el delincuente ajusta en el desarrollo de la condición de operación del ilícito o bien porque se da una adaptación creando un nuevo hacer delictivo ante las políticas de combate o prevención. Esto es la forma más natural en la que el delincuente hace variar el desarrollo del delito ante la presencia de la autoridad o la alerta social. Cuando esto sucede, es muy común que surja el llamado efecto cucaracha, pues los criminales deciden no cambiar su forma de operar sino trasladarse a otro lugar, con características semejantes.

El nuevo lugar elegido por la delincuencia debe tener las condi-

1 Taylor, Ian, Young Jock y otro. *Criminología Crítica.* México, Siglo XXI, 2007, p 235.

ciones anteriores (que le dieron origen al delito (condiciones físicas similares), con ello siguen manteniendo el mismo estatus de riesgo (peligro de ser capturados) y su actividad delictiva genera en promedio los mismos rendimientos. En síntesis esto conduce al traslado del delito en las mismas condiciones de relatividad pero en lugares diferentes con condiciones similares a las que se tenían, por tanto el cambio geográfico no necesariamente cambiaba los *modus operandi*; en ciertos casos estos (modos de acción) se ajustan a la nueva realidad física de ejecución.

Con el paso del tiempo los delincuentes han ido comprendiendo los cambios que se dan en la sociedad y han encontrado formas de ejecutar sus delitos sin cambiar los espacios físicos ni modificar en mucho las formas de actuar, es decir, han logrado adaptarse rápidamente a la sociedad, dejando de lado el efecto de traslado o cucaracha. Pensemos por ejemplo en los lugares urbanos done la vida se va haciendo tan complicada que, en algunos casos el delincuente no necesita ya ni siquiera del efecto traslado, basta cambiar sus hábitos de operación para engañar a las autoridades disfrazando su forma de trabajar y en algunos casos aumentar el número de víctimas en su favor.

El ritmo de la sociedad también se ve modificado desde el ciberespacio. Resulta que prácticamente existe de manera natural otra realidad, paralela al mundo físico, ese lugar es sin duda el ciberespacio. Hoy prácticamente todo lo podemos hacer a través de las tecnologías de la información y la comunicación, esto que la vida cotidiana se puede realizar en el espacio virtual, hacemos negocios, transferencias bancarias, nos comunicamos, todo, consecuentemente, en este lugar debe de existir un resguardo jurídico para los bines que en él se exponen (se arriesgan o se pueden dañar) pero también, para nuestra identidad, nuestros vínculos y nuestras prácticas.

Al igual que en el mundo físico las personas podemos estar en riesgo y exponernos a sufrir daños de todo tipo. El espacio virtual, facilita que el delincuente haya incrementado su actividad básicamente en delitos patrimoniales que son muy comunes por la cantidad

de transacciones que se dan en la red, pero también y de forma muy grave, los delitos respeto de las personas, aprovechando las ventajas que dan ciertos medios tecnológicos. Estas ventajas básicamente son el anonimato y el engaño. "El límite de la sociedad es el mundo y el mundo es el horizonte de las posibilidades, el horizonte dentro del cual lo que es posible puede siempre ser actualizado"[2].

Las victimas más comunes para la comisión de delitos personales atienden a tres características: primero, la vulnerabilidad, nos referimos a personas que aún o alcanzan plena capacidad (menores); segundo; ignorancia, que ligado a la vulnerabilidad aumenta exponencialmente los riesgos. En este punto nos referimos básicamente al factor sorpresa, elemento indispensable para la comisión del delito, hecho que suele también incrementarse en las cuestiones tecnológicas y sus usos, cuando hablamos de sectores de la población que, por la edad, la condición social y económica tienen poco contacto con la realidad virtual; en este clasificación encontramos a los más vulnerables, la personas de la tercera edad, gente sin internet y a dispositivos electrónicos con inadecuada o falta de capacitación y actualización. Tercero; Derivado de las exigencias que de forma sutil va imponiendo el uso de la tecnología para hacer frente a servicios públicos y privados (esto en relación a los puntos anteriores), encontramos a los curiosos que se ligan con desconocidos, se ven sorprendidos por ofrecimientos fascinantes, datos curiosos, remembranzas y en particular lugares de citas o conexiones personales.

Desafortunadamente, los tres puntos de incidencia en delitos cibernéticos tienen que ver en mucho con delitos graves como las redes de trata de personas. En este caso los componentes son los mismos que buscan físicamente en este delito, vulnerabilidad, necesidad de, carencias, soledad, incomprensión, etcétera. Cada una de las necesidades por las cuales las personas se vinculan a estos

2 *Apud. De Giorgi,* Rafael. En: Sánchez, Sandoval (Coord). *Seguridad Pública y la Teoría de los Sistemas en la Sociedad del Riesgo*. México, Porrúa, 2007. P 47

delitos. Esto facilita la fragmentación del delito, pues el enganche de una persona vulnerable y su relación con el mundo físico se dá porque la acción delictiva se parte en muchas formas para cumplir su fin.

Para lograr la conexión con la persona seleccionada basta un principio básico la observación y el manejo de la información del usuario. Lo sorprendente aquí, es como diría *Bauman*[3], uno entra al propio redil de la observación permanente y abre la puerta invitando al delincuente. Evidentemente el medio comisivo cualquier red social, gestó bajo nuestra autorización un espacio para el asecho y el riesgo.

La complejidad entonces está en cómo controlar los delitos que se esparcen y fragmentan con tal velocidad, apareciendo y desapareciendo en un espacio donde todo puede tener sentido o perderlo en un instante. En ciberespacio hasta hoy únicamente existen ciertas rutas formales del control social y muchas de ellas no evitan ser vulnerado, sino como diría *Luhmann*[4], sólo reducen la complejidad delictiva.

Esto es así porque en la dimensión del todo social se incluye el ciberespacio donde todo se conecta y donde interactuamos, por tanto y por antonomasia está presente el delito. Las causas que motivan al ciberdelito pueden ser vistas desde la causa que lo permite (ocasión hace al ladrón) hasta la causa que lo advierte y ataca al mismo tiempo, pero seguro es que no lo eliminará porque encuentra también una dimensión física y otra virtual.

Los escenarios físicos y virtuales, por consecuencia duplican los efectos del mismo, y el control debe de hacer lo mismo; la diferencia

3 Cfr. Zygmunt, *Bauman y Lyon David. Vigilancia Líquida.* España, Paidós. 2017.

4 "*Reducción de la complejidad* es, pues, la palabra clave en el texto *Study of Thinking,* Y ahí se entiende básicamente desde la perspectiva de la *generalización* en dos sentidos: a) el sistema desarrolla un modelo de reacción igual, frente a datos distintos provenientes del entorno, y b) a un mismo estimulo proveniente del entorno el sistema puede reaccionar de diversa manera, dependiendo del estado actual en el que se encuentre. (sic), *Apud, Luhmann, Niklas. Introducción a la Teoría de Sistemas*. México, Universidad Iberoameriacana, 2007 p 181.

estriba en que el ciberdelito puede darse únicamente por esa vía, o por la vía física o por ambas además de establecer como ya se dijo un patrón de concurso de delitos. Se puede afirmar que algunos ciberdelitos, relacionados con el medio físico, resaltan dos momentos, el primero, que en la red, únicamente detectan y vulneran a la víctima a través de información que ella permite, entrega o descuida. Después se da una correlación en el mundo exterior (llamémosle así al físico) donde se constata la información, la vulnerabilidad para después proceder.

La fase de constatación de la información entre el mundo físico y el ciberespacio requiere de organización y de gente capacitada, es por eso que este tipo de delincuentes son muy peligrosos. La forma de desarrollo del delito al exterior es complejo y participan una red de operadores particularmente cuando se trata de delitos contra las personas (trata).

El ámbito de acción de estos criminales es global, pues no sólo se trata de explotar personas y venderlas, se trata de redes multinacionales y eso requiere de sujetos activos a toda escala respecto de la autoría y participación.

> Las tecnologías no solo influyen y cambian la trata de personas y el tráfico ilícito de migrantes, sino también otras formas del delito organizado, como el tráfico de drogas o productos médicos falsificados, entre otros. Cada vez con más frecuencias, estas actividades se realizan en los mercados web (a menudo en la web oscura) en lugar de los mercados físicos. De la misma manera, las tecnologías y la globalización también han sido acompañadas por el establecimiento de nuevas estructuras del delito organizado, que no requieren contacto físico entre el proveedor y el cliente, ni entre los miembros de las organizaciones criminales"[5] (sic).

Los tratantes de personas son considerados delincuentes muy versátiles en los usos tecnológicos pues saben bien, que muchas de

---

5 Doc. Ver. *"Vinculaciones entre la Ciberdelincunecia, el tráfico ilícito de migrantes y la trata*

sus víctimas son niños jóvenes y señoritas en edad adolescente. Para poder estar en contacto con ellos requieren de idear fachadas confiables para poder hacer creíble el mundo virtual y su relación con el mundo físico. Otro ejemplo de la diversificación operandi se da por ejemplo con migrantes, pues el medio virtual es la forma más fácil de enganche tal como se ejemplifica en la siguiente cita:

> Los seres humanos se consideran un producto fuera de línea y en línea (Maras, 2016; Maras, 2018). Con fines de lucro, los tratantes anuncian a los seres humanos y los servicios que pueden proporcionar, buscando clientes que compren estos servicios. Estos tratantes se anuncian en *clearnet* (la *web* visible) y la *deep web* (la web profunda). … Los traficantes utilizan tecnología de la información y la comunicación para proporcionar información y / o comunicar servicios logísticos, tales como tipos de servicios ofrecidos, horarios, fechas y precios de los servicios, opciones y planes de viaje, y artículos, suministros y cualquier equipo necesario. También se puede utilizar para realizar investigaciones sobre rutas de migración[6]. (sic).

Como puede apreciarse, delitos como la trata y la migración se diversificación rápidamente en su *modus operandi*, y se valen de estrategias de innovación tecnológica y de políticas de control delito en sus dimensiones dentro y fuere de la red. Consecuentemente es necesario no solo formas de control y de prevención sino también de incriminación legal, hecho que debe significar que los legisladores tomen en cuenta criterios de actuación policial en la red para recabar evidencia y tener medios de prueba que hoy no están del todo claros en la ley escrita y que en cierta medida es así

Uno de los principales problemas respecto de los controles para la trata de personas menores de edad en la red tiene que ver con la definición, uso, y regulación de los medios tecnológicos.

---

de personas. Trata de Personas y tráfico ilícito de migrantes 14".Declaración de DOHA, UNODC, Educación para la justicia. P3. Fuente electrónica: https://www.unodc.org/documents/e4j/tip-som/Module_14_-_E4J_TIP-SOM_ES_FINAL.pdf Citado el: 23 enero, 2020.

6 *Ibid*, Pp 16-21

III. REDES SOCIALES Y MEDIOS TECNOLÓGICOS EN LA COMISIÓN DE DELITOS

En México no existe un dispositivo legal que nos brinde una definición clara y concreta de lo que debemos de entender por medio tecnológico, dejando a la interpretación lo que pudiera implicar, por lo que para darnos una mejor idea comenzaremos a definirlo palabra a palabra y de esta forma ser conscientes de los alcances que puede llegar a tener.

Por lo que entenderemos al "medio" como todo aquel recurso que nos permite en caso de necesidad, conseguir lo que se pretende; por otro lado, para entender el apartado de "tecnológicos" tendremos que conocer algunos conceptos adicionales ya que el mismo significado hace referencia a la tecnología.

Tecnología, según el diccionario de la real academia española se entiende como "el conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico, es decir el conjunto de conocimientos que estarán ordenados de forma científica, con los cuales se podrá diseñar y crear bienes y servicios, los cuales a su vez facilitaran la satisfacción de las necesidades del ser humano"[7].

Por lo que podemos concluir que el medio tecnológico se entenderá como todos aquellos recursos que nos facilitan y/o permiten el acceso a la tecnología, ya sea por medio de aparatos y/o dispositivos, como lo es un celular o una computadora hasta un programa o aplicaciones.

En la actualidad la tecnología juega un papel muy importante en la vida cotidiana del ser humano, puesto que su desarrollo ha llegado a tal punto, que actividades que antes eran exclusivas del hombre

7 De conformidad con lo que establece el diccionario de la real academia española en su versión en línea 23° ed. actualizada del año 2019; tecnológico, (ca) deviene del griego τεχνολογικός technologikós, siendo entonces su significado el de perteneciente o relativo a la tecnología. Tomado de https://dle.rae.es/tecnol%C3%B3gico, el 15 de noviembre del 2020

ahora son realizadas por maquinas, con ellas se ha buscado tanto el simplificar el uso de la fuerza de trabajo, como del ahorro del tiempo trayendo consigo como consecuencia que actividades como la comunicación sean cada vez más fáciles, hoy en día los usos y aplicaciones de la tecnología, están inmersos en muchos ámbitos de la vida, ya que la gran mayoría de las actividades que desarrollamos a lo largo del día implican el utilizar algún medio tecnológico.[8]

Este desarrollo desmesurado de medios tecnológicos, aunados a la revolución digital de las TIC'S[9], han traído como consecuencia la aparición de un sinfín de plataformas que tienen como finalidad, el libre flujo de la información en todo el planeta, como lo es el Internet, una red de redes que permite la interconexión entre computadoras.

Con el fin de satisfacer esta necesidad del hombre por mantenerse informado y en constante comunicación, surgen disciplinas que buscaran que estas aplicaciones tecnológicas logren su máximo potencial, por mencionar algunas tenemos a la cibernética, informática, el derecho informático entre otras.

Es entonces que con la finalidad de regular los efectos jurídicos que surgen de la interacción entre el derecho y la informática, surge el derecho informático[10], entendiéndolo como el conjunto de principios y normas que regulan los efectos jurídicos nacidos de dicha interacción es decir la relación derecho, hombre y TIC'S.

---

8 La tecnología llega a ser muy ventajosa y provechosa en más áreas de lo que podemos imaginar, áreas, ya que nos permite mejorar la organización en nuestras vidas, la gestión de muchos procesos, ofrecer y recibir más y mejores servicios, en general la tecnología se ha visto inmersa en la gran mayoría de las áreas de la vida cotidiana, muchas veces sin darnos cuenta de ello, estos productos mejoran significativamente la calidad de nuestras vidas, pero como suele pasar en la gran mayoría de las veces, no solemos hacer un uso correcto de ellos , es por eso que resulta necesario ser conscientes de que debemos ser más responsables al utilizarlos, para que dichos avances tecnológicos sean de utilidad y en gran medida evitar causar perjuicios con ellos.

9 Tecnologías De La Información y las Comunicaciones.

10 Es la rama del derecho que se va a especializar en la materia informática, sus usos

El gran avance en los usos de la tecnología trae consigo que surjan nuevas formas de realizar actividades cotidianas, incluyendo a su vez que también las formas de delinquir cambien, estas conductas que van en contra del derecho y las buenas costumbres, entendidas como toda acción u omisión, antijurídica, típica, culpable y punible.

Por lo que concierne al delito informático[11], de acuerdo con lo descrito por el autor Julio Téllez Valdés en su libro Derecho Informático[12], este tipo de delitos tiene como características el que sean conductas criminales de cuello blanco, ser ocupacionales, de oportunidad, provocan serias pérdidas económicas, ofrecen facilidades de tiempo y espacio, son muchos los casos y pocas las denuncias, debido a la falta de regulación jurídica, son muy sofisticados, presentan grandes dificultades para su comprobación por su carácter técnico, en su mayoría son dolosos aunque también hay muchos de carácter culposo o imprudenciales, ofrecen facilidades para su comisión y tienden a proliferar cada vez más.

En México, se ha legislado en torno a esta materia tanto a nivel federal como a nivel estatal, por lo que después de analizar las disposiciones legales aplicables tales cómo el Código Penal Federal y el de algunos estados, podemos establecer, cuáles son los delitos que se contemplan en nuestro país:

a) Acceso ilegal a equipos electromagnéticos;
b) Alteración de medios de identificación electrónica;
c) Fabricación y adquisición, posesión y utilización ilegal de equipos o dispositivos electromagnéticos;
d) Sustracción, uso y revelación de información electrónica confidencial;
e) Defraudación electrónica;
f) Descifrar una señal de satélite cifrada; y

---

y aplicaciones además de las implicaciones legales.

11 El delito informático es toda aquella acción (u omisión) típica, culpable, antijurídica y punible, que se realiza en el entorno informático y está sancionado con una pena.

12 Téllez, Julio. *Derecho Informático*. Ciudad de México, Mac Graw Hill. 2008, P188.

g) Intercepción, interferencia, recepción, alteración, duplicación, reproducción, expedición, sustitución, daño, destrucción y uso indebido de archivos oficiales computarizados o de soportes lógicos o programas de computadoras.

A su vez una red en el sentido amplio es una estructura social, formada por personas o entidades relacionadas entre sí por algún tipo de relación o interés en común; por lo que entenderemos a una red social en internet (*online)* como aquellos sitios de internet formados por un conjunto de individuos que comparten intereses o actividades en común, estas permiten el contacto entre ellos de manera que puedan intercambiar información y comunicarse, sin que necesariamente los individuos que interactúan se conozcan con anterioridad al contacto.[13]

El acceso a este tipo de redes sociales es muy fácil ya que simplemente se necesita llenar un formulario en con datos personales, los cuales podrán ser o no veraces y de esta forma obtener un nombre de usuario y una contraseña.

Las redes sociales son tan sólo una pequeña parte de la social media. De una manera sencilla, son las plataformas sobre las que interactúan y socializan personas y comunidades, con el fin de compartir ideas, noticias e intereses en particular, estas redes permiten compartir una gran cantidad de información de los usuarios, que va desde la que ellos proporcionan al crear su cuenta, como la que la plataforma recaba.

Estas características vulneran a los usuarios, ya que en su gran mayoría las personas hacen un mal uso de las redes sociales, a pesar de los reiterados avisos que se les hacen en cuanto a las medidas de seguridad y recomendaciones para lograr un uso adecuado.

---

13 El estudio del año 2018 de "Redes sociales" que realiza la *Interactive Advertising Bureau* nos dice que podemos definir a las redes sociales *on-line*, como estructuras sociales compuestas por un grupo de personas que comparten un interés en común, relación o actividad a través de internet, donde tiene lugar los encuentros sociales y se muestran las preferencias de consumo de información, mediante la comunicación en tiempo real.

La interacción en las redes sociales son parte de los actividades cotidianas de la gran mayoría de las personas ya sean adultos como menores participan activamente en más de una. Estas plataformas son servicios de Internet que permiten a los usuarios generar un perfil público o privado, en el que pueden plasmar datos personales e información de distinta índole, tal es el impacto y el desarrollo que han alcanzado, que el uso de internet es primordialmente para hacer uso de las redes sociales. Sin embargo, a partir de su uso constante, los usuarios quedan susceptibles a ser víctimas de un sinfín de amenazas informáticas que pueden atentar contra sus datos personales, privacidad, dinero e incluso su propia integridad, logrando salir del mundo virtual al mundo físico.

En general las redes sociales hacen del conocimiento de los usuarios, ciertos mecanismos con los que pretenden regular las interacciones y el contenido que se puede encontrar en estas, dichos mecanismos están al arbitrio del empresario, puesto que en México no hay leyes que regulen los mínimos de seguridad que estas empresas deben de brindar a los usuarios.

Al ser tan fácil el acceso a estas, se resalta la importancia de que los sujetos que acceden a estas plataformas conozcan las medidas de seguridad que se prevén y que el usuario sea consciente de los riesgos que implica el uso de estas plataformas, así como las prácticas que debe de llevar acabo para hacer un buen uso y evitar la mayor cantidad de riesgos que sean necesarios.

Es importante que las personas que accedan a las redes sociales conozcan la cantidad de información a la que les darán acceso a los empresarios de dichas plataformas como a los usuarios en general, entre la información que estas plataformas recaban de conformidad con la política de datos que ofrecen al crear una cuenta encontramos:

- La información que proporcionamos (datos personales).
- El contenido y otros datos que se recaban derivado de las interacciones que tienen cuando usan el servicio además de la información relacionada al uso que le das a la plataforma.

- Las acciones de otras personas en conjunto con la información que puedan proporcionar, con el contenido de esta información puede incluir datos de la persona, como cuando alguien te menciona en un comentario, o te etiquetan en alguna fotografía.
- Información que recaban de otras plataformas con las que trabajan en conjunto, como lo es en el caso de "*Empresas de Facebook*".

Los creadores de estas plataformas recomiendan entre otras las siguientes acciones[14]:

- Usar datos reales;
- Crear solo una cuenta (propia o personal) y usarla para fines personales; y
- No compartir tu contraseña, no concedas a otro acceso a tu cuenta, ni transfieras a nadie tu cuenta

Pero a pesar de esto estas son meras recomendaciones y como tal no existe un medio para comprobar ni obligar a que se sigan y lo que es peor que los datos que se introducen sean verídicos.

Como otra medida de seguridad encontramos el restringir el acceso a menores de 13 años; a delincuentes condenados por delitos sexuales; por la inhabilitaron previa de su cuenta por incumplir las condiciones o políticas y cuando las leyes aplicables prohíban que recibas los productos, servicios o *software*.

Respecto de los menores de edad haciendo uso de los medios tecnológicos y de las redes sociales mencionaremos que los menores de edad son los que mayor acceso tienen a las redes sociales y por ende su interacción con la tecnología empieza cada vez a más temprana edad, dicha situación presenta grandes oportunidades, pero

---

14 Los creadores de páginas como Facebook suelen hacer recomendaciones a los usuarios acerca de cómo hacer un uso correcto de ella; estas recomendaciones las podemos encontrar en las políticas y condiciones de uso, así como en el buzón de ayuda de la plataforma, éstas recomendaciones tienden a implementar acciones que son encaminadas a vigilar el cumplimiento de las normas comunitarias que tienen como finalidad el generar un entorno seguro para los usuarios de estas plataformas tomado de https://es-es.facebook.com/about/privacy, 3 diciembre del 2020

también los expone a grandes riesgos.[15]

El auge de los teléfonos celulares y dispositivos portátiles ha facilitado la conexión constante desde cualquier lugar, permitiendo que los jóvenes se conecten de forma más privada y sin supervisión, lo que los deja más vulnerables y susceptibles a ser víctimas de cualquier delito cometido en estos medios tecnológicos y redes sociales.

En internet, los niños pueden acceder fácilmente a todo tipo de contenido incluyendo el contenido inadecuado para ellos, como imágenes violentas o pornográficas. Padres e hijos a menudo no son conscientes de los grandes riesgos que supone el compartir datos personales en la red. Ya que estos exponen a los menores a la amenaza de acosadores, traficantes y otras personas que quieran hacerles daño. Además, de que en el mundo digital los acosadores y en general las personas que delinquen gozan de mayor anonimidad.

La tecnología puede hacer que los niños sean más susceptibles de sufrir daños tanto en línea como fuera de ella, puesto que las TIC'S están intensificando los riesgos habituales de la niñez, como bien lo es la intimidación, y de esta forma fomentan nuevas formas de delinquir y vulnerar los derechos de los menores, siendo más fácil el contacto con ellos, ya que los depredadores pueden comunicarse de forma más sencilla con niños a través de perfiles "falsos" en las redes sociales y en general por cualquier otro medio tecnológico sin contar con protección alguna.[16]

En México, las estadísticas disponibles sobre el delito de trata de personas son muy escasas y para algunos estados del país simplemente no hay información lo cual a su vez dificulta que se pueda

---

15 Dicha conclusión surgió a partir del informe "*El Estado Mundial De La Infancia 2017: Niños En Un Mundo Digital*", donde la UNICEF analiza por primera vez los efectos positivos y negativos de la tecnología en la vida cotidiana de los niños. Tomado de https://www.unicef.org/spanish/publications/files/SOWC_2017_SP.pdf 20 de noviembre del 2020

16 Ante este escenario de amenazas, el uso de redes sociales puede parecer peligroso. No obstante, si se siguen ciertos criterios y buenas prácticas, es posible utilizarlas y contar con niveles de protección para un uso correcto y seguro de estas plataformas, para que de esta forma se pueda explotar el al máximo los beneficios de estas plataformas.

dimensionar el problema y los alcances que este tiene, por lo que es difícil que también se puedan implementar medidas que realmente ataquen el problema.[17]

El uso de las nuevas tecnologías de la información, particularmente hablando en el caso del Internet, podemos decir que este ha adquirido en los últimos años gran relevancia para la captación de las víctimas por el crimen organizado, pues se estima que el internet está presente en uno de cada cinco casos de trata. [18]

Tenemos que encontrar el punto medio que brinde armonía con tantos avances tecnológicos existan, pero siempre sin perder el sentido de lo realmente importante, sin olvidarnos de que las personas que conocemos en las redes, no necesariamente son reales o son quien dicen ser, a esto debemos sumar que no todas las personas que navegan en estas plataformas tienen buenas intenciones, aunado a que la ampliación de la finalidad de estas plataformas trae consigo la posibilidad de que se cometan más delitos como el fraude, el robo de información o identidad etc., puesto que no todo lo que vemos en internet es real, lo que conlleva uno de los problemas más grandes que encontramos en estas plataformas las *fake news,* la plaga de la información falsa en internet, con lo que podríamos concluir que estamos pasando a ser de la sociedad de la información, a la sociedad de la desinformación.

Al comenzar a ser conscientes del contenido personal que compartimos en las redes sociales ya sea través de publicaciones, de mensajería o cualquier medio que estas plataformas nos ofrecen podemos evitar muchos riesgos, porque lo que está en Internet en Internet se queda, aunque lo borremos o intentemos que desaparez-

---

17 *Cfr.* Programa Nacional para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y Para la Protección y Asistencia a las víctimas de estos Delitos. 2014-2018.

18 Dato obtenido de la Comisión Nacional de los Derechos Humanos .2013, en la primera edición del Diagnóstico sobre la situación de trata de personas en México. Tomado de https://www.senado.gob.mx/comisiones/trata_personas/docs/Diagnostico_Trata.pdf 10 de noviembre del 2020

ca, la huella digital que deja es para siempre.

Se trata de no hacer en el mundo digital lo que no haríamos en el mundo físico, ser más críticos con el contenido que compartimos y verificar las fuentes que lo han compartido, puesto que como hemos intentado destacar *supra,* un uso erróneo de estos nos puede llevar a ser víctimas de algún delito.

IV. TRATA DE MUJERES MENORES DE EDAD

El protocolo Palermo[19] prevé un concepto para el delito de trata de personas por lo cual se entenderá en términos de este, como la captación, el transporte, el traslado, la acogida o la recepción de personas, recurriendo a la amenaza o al uso de la fuerza u otras formas de coacción, al rapto, al fraude, al engaño, al abuso de poder o de una situación de vulnerabilidad o a la concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra, con fines de explotación. (Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, ONU, 2000)

Dicha explotación incluirá, cuando mínimo, la explotación que se derive de la prostitución ajena u otras formas de explotación sexual, los trabajos o servicios forzados, la esclavitud o las prácticas análogas a la esclavitud, la servidumbre o la extracción de órganos. Incluyendo que el consentimiento dado por la víctima de la trata de personas no se tendrá en cuenta, cuando se haya recurrido a medios como las amenazas o el uso de la fuerza incluyendo otras formas de coacción, el rapto, el fraude, el engaño, el abuso de poder o de una

---

19 *Cfr.* De conformidad con el portal de la Fiscalía General de la Republica, éste documento fue ratificado en México el 25 de diciembre de 2003 y su nombre completo es el "Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional". Tomado de https://www.gob.mx/fgr/es/articulos/conoces-el deprotocolopalermo?idiom=es#:~:text=Fue%20ratificado%20por%20M%C3%A9xico%20el,contra%20la%20Delincuencia%20Organizada%20Transnacional. 10 de noviembre del 2020

situación de vulnerabilidad sin dejar de lado a la obtención o recepción de pagos o beneficios que dicha situación le pudiera generar.

Sancionando de igual forma la captación, el transporte, el traslado, la acogida o la recepción de un niño con fines de explotación se considerará de igual forma como trata de personas, incluso cuando no se recurra a ninguno de los medios enunciados en el párrafo anterior, los cuales están establecidos en el protocolo y finalmente delimita quienes serán considerados niños para fines de aplicación del instrumento por lo que por "niño" se entenderá a toda persona menor de 18 años.

Derivado de lo plasmado en este instrumento es que México al firmar y ratificarlo, se da a la tarea de crear instrumentos que se apeguen a lo que se establece en el protocolo Palermo, dando así una concepción allegada a estos lineamientos.

Por lo que el concepto que la ley mexicana nos brinda es el de toda acción u omisión dolosa de una o varias personas para captar, enganchar, transportar, transferir, retener, entregar, recibir o alojar a una o varias personas con fines de explotación, agregando en esta definición que actividades serán consideradas como explotación con su debida penalidad.[20]

En ella se contemplan once modalidades de explotación dentro del delito de trata de personas siendo los siguientes: esclavitud, condición de siervo, prostitución ajena u otras formas de explotación sexual, explotación laboral, trabajos forzados, mendicidad forzada, uso de menores en actividades delictivas, adopción ilegal de menores, matrimonio forzoso, tráfico de órganos y experimentación biomédica.

El delito de la trata de personas es uno de los delitos más lucrativos a nivel mundial, justo por debajo del narcotráfico, en donde se estima que 1 de cada 4 víctimas son menores de 18 años. La organización internacional de trabajo (OIT) considera que en el 2016, 40.3 millones de personas estuvieron sometidos a la trata de

20 Ley General Para Prevenir, Sancionar Y Erradicar Los Delitos En Materia De Trata De Personas Y Para La Protección Y Asistencia A Las Víctimas De Estos Delitos, concepto se encuentra en el artículo 10.

persona.

Este delito afecta principalmente a las mujeres y niñas, de las cuales, según la Secretaria de Gobernación de nuestro país, el 99 por ciento de estas son vinculadas a la industria sexual comercial.

El diagnostico nacional sobre la situación de trata de personas en México, realizado por la *United Nations Office on Drugs and Crime* (UNODC)[21], a grandes rasgos señala quienes son los grupos son más vulnerables y por ende que están más propensos a ser víctimas de este delito, teniendo como factor en común las victimas el ser aquellas que sufren de exclusión y de discriminación, que viven condiciones de vulnerabilidad socioeconómica de carácter sistemático y/o que sufren de carencias afectivas o emocionales. En este sentido, el perfil de las víctimas identificadas, en conjunto con distintos indicadores económicos y sociodemográficos, confirman que las mujeres, particularmente las niñas, adolescentes y jóvenes, son las más susceptibles a ser víctimas de este delito.

Por lo que se puede deducir que esto se debe a que en nuestro país, como en muchos otros, este grupo es el que más sufre de la inequidad del acceso a la educación, trabajo y estereotipos de género, que a su vez las vuelven un objeto de cambio.

Son las mujeres y particularmente las niñas, adolescentes y jóvenes las más susceptibles a ser víctimas del delito de trata influyendo en esta situación factores, como la pobreza, desempleo, falta de acceso a servicios básicos, la pertenencia étnica o racial, el conflicto armado, entre otros los que facilitan de cierto modo que las mujeres y otras personas de determinados grupos sean más propensas a enfrentar esta forma de violencia.

Sobre el *modus operandi* de los tratantes, se han identificado algunos patrones recurrentes, como el enganche por engaño que consiste en la desvinculación de la víctima de sus redes sociales y familiares,

---

21 *Cfr.* UNODC, Diagnóstico Nacional sobre la Situación de Trata de Personas en México, 2014. Obtenido de https://www.gob.mx/cms/uploads/attachment/file/37682/Diagnostico_UNODC.pdf 15 de noviembre del 2020

estrategia que los tratantes utilizan para someterla, para cualquiera que sea la finalidad de la trata a la que serán sometidas las víctimas.

Los grupos y redes criminales que se dedican a este delito presentan cambios constantes en sus estructuras delictivas, los cuales aprenden, innovan y adaptan, puesto que con la evolución de la tecnología surgen nuevas herramientas, como el Internet, que pueden potenciar el *modus operandi* de los tratantes y facilitar el reclutamiento de víctimas por estos medios.

Es importante decir que la trata de personas, es uno de los delitos que más se intenta minimizar ya que en la población en general no hay conciencia acerca de ello, aunado a la falta de capacitación de servidores públicos como lo son los policías, ministerios públicos y jueces para una adecuada investigación y procesamiento de los delincuentes, además de que es necesario actualizar las leyes que prevén estos delitos, para brindar mayor protección a todos aquellos que pueden ser víctimas de este delito, puesto que en nuestro sistema al no haber un adecuado trato a las víctimas, se desalienta la denuncia, dejando múltiples lagunas jurídicas al no existir datos que prueben que existe falla en las leyes.

Con el acelerado desarrollo de las tecnologías, la facilidad con la que se puede acceder a la información de cualquier tipo y el absoluto poder de la informática, los campos de acción de los delincuentes se amplió aún más, como lo hemos visto en párrafos anteriores es muy fácil tener acceso a las redes sociales por lo que no toda la información que encontramos en ellas es fidedigna, por lo que a pesar de que en la mayoría de las redes sociales no se permite el acceso a menores edad es muy fácil que estos y cualquier otra persona creen una cuenta con datos falsos, solo por tener acceso a estas.

El internet abre un mundo de información para todos y todas, pero debemos de contar con información para un adecuado y responsable uso, para evitar ser víctimas de delitos puesto que con esa gran apertura a las conexión y acceso a la información, también se amplió el campo de acción de los delincuentes.

Las redes sociales resultan un medio conveniente para que cualquier persona enganche a niñas, niños y adolescentes con falsas esperanzas, promesas de una vida mejor o manipulándolos sentimentalmente, son un medio conveniente para enganchar menores de edad, puesto que en la red todos pueden ser lo que quieren, sin el temor de que los juzguen por ello, en donde puedes conocer gente con la que compartes intereses y que de cierto modo los comprende, además del acceso ilimitado que les dan a su información personal.

A través de las redes sociales y de toda la información que el usuario hace pública, la personas en general pueden saber toda clase de información desde, en que escuela estudia, con que personas interactúa, en qué lugares suele estar, se puede llegar a intuir también la situación económica, sin hablar de los intereses, y de más información que pueda facilitar a todos los demás usuarios.

Así mismo La Fiscalía Especial para los Delitos de Violencia Contra las Mujeres Y Trata de Personas dice que los tratantes enganchan a sus víctimas ya sea por ofertas prometedoras de trabajo, o de cualquier otro tipo en donde se le ofrecen todo tipo de cosas que la persona pueda desear, o buscan personas vulnerables en las redes sociales, compartiendo intereses con la víctima y así ganando su confianza apoyándolos en sus ideas, se hacen amigos de las víctimas y les piden conocerse personalmente, para posteriormente ser vinculadas a la trata.

Los menores de edad son un grupo vulnerable, se estima que el 51% de los usuarios son mujeres y el 21% de ellos se encuentran entre los 12 y 17 años, utilizando un promedio de ocho horas un minuto el internet, siendo la principal actividad que se realiza en el internet el acceder a redes sociales, además de que Facebook se considera es la principal plataforma usada en el país.[22]

De ahí la gran importancia que están tomando estas en nuestro país, puesto que día con día en estas se pueden hacer más cosas,

22 Asociación de Internet MX en su 13° "Estudio Sobre Hábitos De Los Usuarios De Internet en México" (2017) P. 5. Tomado de: https://irp-cdn.multiscreensite.

no solo conocer gente sino que ya podemos hacer un sinfín de actividades como lo es el comprar/vender cosas, además de que las empresas están actualizándose dado al avance tecnológico y ponen su publicidad en estas ya que los anuncios en tv o radio ya no son tan vistos por el auge de otros medios de comunicación.

Los Smartphone son el principal dispositivo para acceder a alguna red social, puesto que 8 de cada 10 internautas utilizan estos dispositivos, trayendo consigo que en consecuencia el crecimiento de usuarios sea mayor, puesto que con estos dispositivos también se facilita el acceso a internet prácticamente en cualquier momento y en cualquier lugar, facilitando de esta forma el hecho de ser rastreados en tiempo real, con lo que es más fácil saber que lugares frecuenta alguien, con quien, en donde vive, en donde estudia etc.[23]

Estas plataformas también son utilizadas por los explotadores para ofrecer al público como mercancía a las personas captadas, difundir y comercializar los materiales derivados de la trata, como la pornografía en grupos creados en estas plataformas, reforzando nuestro punto de que las medidas de seguridad de estas resultan insuficientes para garantizar la integridad de los usuarios, permitiendo este tipo de grupos pudiendo pasar mucho tiempo sin que se percaten de estas conductas.

Además de que los pederastas y turistas sexuales utilizan internet para planear o concertar encuentros sexuales con personas que son explotadas, esto con las facilidades que el internet les brinda puesto que en estas plataformas sociales es difícil poder asegurar que la información que una persona entrega a estas es verídica, desde su identidad, hasta los datos personales o de cualquier índole que comparten.

---

com/81280eda/files/uploaded/ocde.pdf, 4 de diciembre del 2020

23 Asociación de Internet MX en su 13° "Estudio Sobre Hábitos De Los Usuarios De Internet en México"(2017), P 11, tomado de https://irp-cdn.multiscreensite.com/81280eda/files/uploaded/13_Estudio_Habitos_del_Usuario_2017.pdf, 4 de diciembre del 2020

De este modo, Internet ha pasado a formar parte del proceso de la trata de personas, por lo que se insiste, sobre todo a padres de familia y a adolescentes a ser cautelosos ya sea con la supervisión para los primeros y el manejo de información y contactos con los segundos, ya que bastaría con navegar unos momentos en cualquier red social para darse cuenta de la cantidad de irregularidades, contenidos y usuarios no cumplen con las normas que las mismas plataformas ponen.

Resulta de suma importancia el concientizar a la población de los riesgos que se pueden enfrentar al hacer uso de estos y como hacer un uso adecuado de las redes, aunado a una legislación que obligue a ofrecer ciertos mínimos de seguridad a los usuarios.

V. PREVENCIÓN TECNOLÓGICA.

Las medidas de seguridad que ofrecen las redes sociales son por decirlo de una manera, son una mera recomendación, las cuales carecen de coercibilidad para exigir su cumplimiento a los usuarios, dejando una brecha, con la cual se facilita el que se realicen ciertas conductas, las cuales van en contra de lo que se considera correcto y de las buenas costumbres, que van desde el simple hecho de compartir contenido inadecuado, hasta la comisión de delitos.

Estas medidas no ofrecen la certeza al usuario de que las personas con las que interactúa son quien realmente dicen ser y de que la información que circula por estos medios es verdadera, resultan ser insuficientes para ofrecer un mínimo de seguridad, puesto que estas plataformas sociales a lo largo de su evolución, han ido ampliado su finalidad, que en un principio era la de conectar o conocer personas y en la actualidad además de esa finalidad se llegó al punto en el que se pueden vender productos, hacer ofertas de empleo, hasta la de promocionar ya sea empresas, productos o personas entre muchas otras que día a día se van incluyendo.

Resultará entonces necesario el establecer medidas de seguridad en las redes sociales, además de lograr que la población esté infor-

mada y consiente de lo que implica el uso inadecuado de las redes sociales y a los peligros a los que se exponen haciendo uso de estas.

Si nos enfocamos a la red social más usada en la actualidad es decir Facebook[24], ellos intentan combatir las conductas perjudiciales, con un equipo especializado que desarrolla sistemas técnicos avanzados para detectar si los productos de la compañía de alguna manera son utilizados de forma inapropiada, además de eliminar contenido, bloquean el acceso a ciertas funciones e inhabilitar una cuenta, de limitar el uso para menores de trece años, para personas que hayan cometido delitos sexuales y hayan sido condenados por ellos o si se le ha inhabilitado previamente su cuenta por incumplir las condiciones o políticas que estas redes sociales establecen.

Ellos recomiendan[25] a los usuarios seguir las siguientes acciones para dar un buen uso y evitar que alguien de cierta forma usurpe su identidad siendo el usar el mismo nombre que usas en la vida cotidiana, brindar información precisa sobre ti es decir verdadera, crea solo una cuenta y usarla para fines personales, no compartir contraseñas y no conceder a otros acceso a tu cuenta de Facebook.

Con esta misma finalidad se crean las normas comunitarias, que surgen por la necesidad de que los usuarios que las utilizan se sientan de cierto modo seguros al navegar por estas y de mantener los abusos lejos de las mismas, estas normas se aplican en todo el mundo por igual, el objetivo primordial de estás es que se fomente que las personas se expresen y creen un entorno seguro.

Cabe mencionar que se insiste a todos los aquellos que hacen uso de esta a que todo el contenido que compartan sea de forma responsable y que si ven algún contenido que infrinja las normas que

---

24 Esto de conformidad con el contenido proporcionado por Asociación de Internet MX en su 13° "Estudio Sobre Hábitos De Los Usuarios De Internet en México" (2017) P.18 Obtenido de https://irp-cdn.multiscreensite.com/81280eda/files/uploaded/13_Estudio_Habitos_del_Usuario_2017.pdf 4 de diciembre del 2020

25 *Cfr.* Refiérase a los creadores de la plataforma de *Facebook* en sus políticas de uso y privacidad así como sus normas comunitarias. . Tomado de https://www.facebook.com/communitystandards/introduction 6 diciembre del 2020

se plasman en la red social, se realice un reporte para que se puedan tomar las medidas necesarias en cuanto al contenido de dichas publicaciones. Estas normas comunitarias versan sobre seis puntos que su vez son la base sobre la cual se estructuran y son: violencia y comportamiento delictivo, seguridad, contenido inaceptable, inseguridad y autenticidad, propiedad intelectual y solicitudes relacionadas con el contenido,

Las medidas que esta plataforma prevé sirven y son muy útiles, pero son insuficientes mientras no sean obligatorias, debido a la naturaleza de las medidas establecidas por las redes sociales, estas quedan al arbitrio del usuario y dependerán en gran medida de que estos las conozcan, puesto que serán estos mismos los que deciden si seguirlas o no, además de que él tiene el control de a quien le permite acceso a la información que ofrece en su perfil.

Es a lo largo de la evolución de los avances tecnológicos y de su ajuste con la vida cotidiana, que han surgido varios intentos de regular estas plataformas por lo que en todo el mundo se abren debates sobre lo que el marco legal aplicable a estas debe de abarcar, se tratan de cuestiones distintas según la región por lo que se tienen objetivos diversos que van desde la protección de la seguridad de los menores de edad, al uso y comercialización de los datos personales, la seguridad de grupos vulnerables, hasta el intento de poner límites a las empresas tecnológicas o censurar los contenidos, sobre todo aquellos de carácter político.

Por lo que se podríamos resumir que dichos debates se centran en los siguientes puntos: protección de datos personales, puesto que los datos personales se han convertido en uno de los bienes más valiosos para las empresas de tecnología, comunicación digital y elecciones, puesto que los procesos electorales se han visto afectados por el uso de las nuevas plataformas sociales, libertad de expresión, regulación de contenidos.

La tecnología se ha convertido en un punto esencial para realizar diversas actividades de la vida social y laboral, entendiendo

que este, es un entorno versátil y dinámico, como en muchas otras ramas, está expuesto a que se cometan delitos a través de ellos.

Es entonces que se entra en la discusión, de si en realidad debe de regularse el uso de las redes sociales y las tecnologías, o solo hacer un uso ético de las tecnologías y dejarlo al arbitrio de los usuarios, por lo que es importante reflexionar sobre la importancia de la aplicación de una actitud ética para el uso de las redes sociales y medios tecnológicos.

La tecnología de la información o TIC'S dan lugar a nuevos aspectos éticos, tanto como para los individuos como las sociedades, porque crean oportunidades para un cambio social, regular las redes sociales no necesariamente debe de implicar el prohibir, por el contrario, la importancia radica en la creación de normas que permitan el ejercicio de los derechos del individuo, incluyendo los digitales con libertad y de esta forma poder evitar abusos.

Se cree complicado y de cierta forma lo es, ya que por una parte existe una minoría selecta, que ha visto a la comunicación digital como una molestia, caótica y difícil de controlar y, por otro lado, es que todos los usuarios de las TIC'S tengan leyes que permitan ejercer sus libertades y derechos y que además les otorguen un mínimo de certeza jurídica relacionado a las medidas de seguridad que estas plataformas deberían de ofrecer, el derecho y la ética, en conjunto, son una herramienta que nos permitirá fortalecer la implementación de estrategias de seguridad en la informática y por tanto en las redes sociales.

La tecnología ya nos ha rebasado y aunque con anterioridad veíamos como algo innecesario el tener que legislar simples y aparentemente inofensivos medios de entretenimiento, sin embargo, hoy en día el derecho parece estar unos pasos atrás cuando se pretende regular la actividad que transcurre en un espacio como Internet, en el que confluye una gran cantidad de información e interactúan miles de personas sujetas además a distintas legislaciones.

Sin embargo, la regulación de las conductas y fenómenos que se

cometen en la red ha sido ineficaz y hasta contraproducente, puesto que impulsa posturas radicales que niegan cualquier posibilidad de regulación, aludiendo a que se transgreden derechos como lo es el de la libre expresión.

Por tanto, es necesario definir al internet y entender su funcionamiento, a efecto de realmente poder valorar qué es lo que hace y no hace, así como cuáles son las verdaderas posibilidades de regularlo y el de establecer mínimos de seguridad para los usuarios de estos.

Resulta muy complicado que la regulación se mantenga al día de cada uno de los avances tecnológicos que se vayan presentando, puesto que estos avanzan a pasos agigantados, siendo tan cambiantes como la naturaleza misma de estos, lo que lo hace difícil de definirla.

Consideramos con base a lo que se expuso en párrafos anteriores, que se tendría que alinear el tipo penal de trata de persona, a las demandas actuales de la sociedad con todos los aspectos que la integran, para brindar protección real a esta y poder combatir el delito, de la misma manera que se intentara prevenir la comisión del mismo.

Ya que en los últimos años se aumentó el uso de la tecnología para delinquir, aprovechando esta falta de regulación o la forma tan burda en que se ha abordado, debe de ser incluida como elemento en el tipo penal y de igual forma incluir en las agravantes cualquier situación que se pueda derivar del mal uso de las redes sociales y medios tecnológicos.

El internet llego a replantear la forma en la que recibimos y procesamos la información, por ende, cómo entendemos y percibimos al mundo. Esta falta de conceptualización de cómo funciona el internet y como afecta a todos los aspectos de nuestras vidas ha llegado a generar que los intentos por regular todo lo concerniente al internet y sus derivados hayan sido ineficaces e insuficientes.

De forma equivocada hemos considerado al internet como un mero sistema de distribución de información que no tiene ningún

tipo de trascendencia en nuestras vidas, lo cual en nuestros días ha quedado superado del todo, puesto que el internet ha evolucionado con tal velocidad y a tal magnitud que en la actualidad, con el uso del internet se pueden hacer muchas cosas, influyendo en todos los aspectos de nuestras vidas.

No obstante, estos cambios y sus consecuencias han sido abordados de una forma muy burda, puesto que se han dejado de lado muchas situaciones en las que se incurren en delitos. En la actualidad el internet se encuentra en todas partes, por lo tanto, su regulación no se puede dar desde la perspectiva de una entidad soberana dentro de un territorio limitado.

Derivado de esta premisa podremos concluir que sería importante para prevenir la comisión de delitos a través de este, la creación de un protocolo que se aplique a las redes sociales, mediante el cual se procure la autentificación de perfiles.

Por lo que entenderemos a protocolizar la autentificación de perfiles, como la secuencia de pasos que cada usuario de la red social debe de seguir para llevar a cabo un proceso mediante el cual se acreditara que el perfil que utiliza en estas, es el propio y es real, procurando de igual forma que este sea obligatoria para todos y cada uno de los usuarios que quieran o tengan acceso a la red social de la que se trate.

En las redes sociales, existe ya un proceso de verificación de perfiles, pero no es un procedimiento del que todos los usuarios conozcan y de igual forma está apegado a una previa solicitud a la plataforma para que esta delibere si es factible que se le otorgue una cuenta verificada o no, por lo regular este proceso de verificación se les otorga a negocios o figuras públicas, cada red social cuenta con su propio y específico proceso a la hora verificar. Con este protocolo combaten a su manera las noticias falsas y también se evita la suplantación de la identidad de sus usuarios por parte de terceras personas.

Sería ideal que las plataformas realizaran un proceso similar para el resto de los usuarios, esto con la finalidad de ver y controlar

quienes tienen acceso a estas, y por supuesto también podría influir para evitar que se cometan delitos en estas o por medio de estas. El realizar este proceso trae consigo muchas ventajas no solo para las plataformas, puesto que las cuentas verificadas pueden proteger la integridad de los propietarios de las cuentas y evitar el robo de identidad como se ha mencionado antes.

Al existir una verificación de perfiles, existiría una protección real a los usuarios, brindando con esta un mayor control y en consecuencia protección a los usuarios ya que se podrían prevenir un sinfín de situaciones que continúan pasando pese a las medidas de seguridad y normas que las mismas han implementado y mejorado a lo largo de los años desde su aparición.

Por lo que consideramos que la creación de un instrumento legal que otorgue las bases que sean el cimiento para la regulación de las medidas de seguridad que ofrecen las redes sociales es en esencia muy necesario en la actualidad. Dicho instrumento deberá como mínimo establecer medidas de seguridad tendientes a:

- Resguardar y vigilar el uso que se le da a la información que proporcionamos a este tipo de plataformas incluyendo desde la que proporcionamos de forma consiente, hasta el contenido al que accedemos y otros datos que se recaban al compartir contenido cuando se usa el servicio.
- Fomentar el uso adecuado que se le da a la plataforma por parte de los usuarios, evitando que se utilice para cometer cualquier tipo de ilícito o compartir información que se pueda considerar sensible, o que lleve a la investigación de cualquier comisión de delitos.
- Brindar la certeza de que se pueda realizar compras, hacer alguna transacción y que los datos sobre la información de pago se encuentren resguardados garantizando que estas no sean utilizadas de manera inadecuada por terceros o por la misma plataforma.
- Combatir la mayor cantidad de conductas perjudiciales, a través de una dependencia, como bien lo podría ser la policía científica de la policía federal, que cuenta con equipos técnicos, que poseen el conocimiento técnico y práctico para poder determinar la comisión

de delitos en medios cibernéticos en nuestro caso particular en las redes sociales.

- Garantizar la veracidad de los datos que se introducen al momento de crear una cuenta como lo son el nombre y la edad, con la finalidad de evitar cuentas falsas, robo de identidad, y de forma muy ambiciosa evitar la comisión de delitos y un mayor control de lo quienes tienen acceso a estas redes sociales.
- Detectar y canalizar todo tipo de actividad delictiva, así como las redes criminales que hoy en día utilizan las redes como medio de comunicación, organización y de enganche para sus fines.
- Lograr que las redes sociales sean un medio en el que las personas que interactúan se sientan seguras y con la certeza de que no corren ningún tipo de riesgo al hacer uso de ellas.
- En general todo tipo de medida que permita otorgar soporte a las normas que estas plataformas ofrecen en sus páginas online, puesto que están bien direccionadas pero carentes de coercibilidad.

Como se ha mencionado, la regulación de las redes sociales, no necesariamente debe de implicar el prohibir, o de coaccionar el derecho de expresión como muchos creen, por el contrario, la importancia radica en la creación de normas que permitan el ejercicio de los derechos del individuo, incluyendo los digitales, con libertad y de esta forma poder evitar abusos y brindar seguridad al usarlas.

Con lo cual de acuerdo con las conclusiones plasmadas en la tesina "Redes sociales y medios tecnológicos como factor de riesgo en la trata de personas, mujeres adolescentes"[26] podemos agregar que en general la mayoría de las personas que tienen acceso a los medios tecnológicos, en específico a las redes sociales *on line*, desconocen cómo hacer un correcto uso de estas lo que conlleva a su vez que en gran medida no conozcan las medidas de seguridad que estas ofrecen a los usuarios y puesto que la finalidad principal con la cual se crearon se ha expandido, trayendo consigo que estas sean

26 Escoto Delgado, Carla María. Tesina "Redes sociales y medios tecnológicos como factor de riesgo en la trata de personas, mujeres adolescentes". Estado de México, UNAM. 2019.

utilizadas por personas que tienen como objetivo el cometer delitos aprovechando la dificultad que representa el perseguir los delitos cibernéticos, trayendo consigo que se vulnere de forma considerable la seguridad de niños y mujeres, ya que por el contexto social que se vive en México estos grupos suelen ser considerados como vulnerables.

Por lo anterior seria de suma importancia que se comience a implementar campañas de información con la finalidad de concientizar a todos aquellos usuarios, de los peligros que se corren al hacer uso de las redes sociales, en donde de igual modo se les dé a conocer cuál es la forma correcta en que deben de usarse y finalmente y después de todos los ajustes legales pertinentes resultaría importante desarrollar toda una estrategia de políticas públicas encaminadas a la prevención del delito por medios electrónicos y en particular del cuidado y asesoría de las niñas que usan la red.

VI. EPÍLOGO

El delito de trata de personas se ha transformado y diversificado del mundo ral, común al virtual. Sus víctimas son todas las personas vulnerables pero más aún los menores, las niñas y los migrantes. Las redes sociales se han vuelto el medio y la herramienta para identificar, monitorear y atacar a las personas. Los delincuentes han logrado con éxito vincular el negocio virtual con el real, haciéndolos imparables; su estrategia es cambiar sus *modus operandi* y sorprender de forma particular a aquellos que por ignorancia, negligencia, descuido o falta de atención pueden ser vulnerados.

Las redes sociales y sus políticas de seguridad van acompañadas de largas advertencias y referencias de acción no claras para todo tipo de usuarios. Las estrategias públicas en espacios privados para prevenir los delitos cibernéticos no existen de forma específica, por tanto ambos terrenos son tierra de ciberdelincuentes. En el mundo de hoy, no tiene sentido las políticas restrictivas en las redes sociales

porque son parte de un mundo globalizado donde la interacción entre personas de todo el mundo a todas horas es ya, inevitable.

Por tanto, es tiempo de pensar que la fórmula tradicional de la prevención debe de ser puesta en marcha desde lo público a lo privado, antes de que una persona decida ingresar a las redes sociales. La instrucción abierta (espacios públicas) desde temprana edad sobre el mundo de riesgos que implica usar una red social con desconocidos o la exposición de información personal al púbico puede ser un acercamiento al delito; ambas acciones son también responsabilidad social compartida con los miembros de la familia particularmente cuando se trata de menores.

Es tiempo que los Estados no solo se preocupen de los magantes de las redes sociales por los intereses económicos, sino también por obligarlos a mejorar y hacer más claras sus políticas de privacidad y señalamiento de riesgos al hacer uso de las plataformas. De forma particular es importante advertir a menores y jóvenes adolescentes que jamás deberán de entrar en contacto con desconocidos y menos vincularse con ellos en el mundo real (exterior). Tal vez se tiempo ya, de que las autoridades también realicen campañas de prevención dirigidas de forma específica a grupos vulnerables como las niñas y las mujeres.

En el mundo virtual todo es posible todo el tiempo, pero nada es posible, si no lo permitimos.

VII. FUENTES DE CONSULTA.

Bibliografía

Escoto Delgado, Carla María. Tesina: *Redes sociales y medios tecnológicos como factor de riesgo en la trata de personas, mujeres adolescentes*. Estado de México, UNAM. 2019

Luhmann, Niklas. *Introducción a la Teoría de Sistemas*. México, Universidad Iberoameriacana, 2007

Márquez Piñero Rafael. El tipo penal. México. UNAM. Instituto de

investigaciones Jurídicas. 1992

Nava Garcés Alberto Enrique. Delitos Informáticos. México. Porrua.2007

Sánchez, Sandoval (Coord.). *Seguridad Pública y la Teoría de los Sistemas en la Sociedad del Riesgo.* México, Porrúa, 2007

Taylor, Ian, Young Jock y otro. *Criminología Crítica*. México, Siglo XXI, 2007.

Téllez, Julio. *Derecho Informático.* Ciudad de México, Mac Graw Hill. 2008

Zygmunt, Bauman y Lyon David. *Vigilancia Líquida*. España, Paidós. 2017.

Fuentes Electrónicas

*"Vinculaciones entre la Ciberdelincuencia, el tráfico ilícito de migrantes y la trata de personas. Trata de Personas y tráfico ilícito de migrantes 14".*Declaración de DOHA, UNODC, Educación para la justicia. P3. Fuente electrónica: https://www.unodc.org/documents/e4j/tip-som/Module_14_-_E4J_TIP-SOM_ES_FINAL.pdf Citado el: 23 enero, 2020.

"*El Estado Mundial De La Infancia 2017: Niños En Un Mundo Digital*", UNICEF. Tomado de :https://www.unicef.org/spanish/publications/files/SOWC_2017_SP.pdf 20 de noviembre del 2020

"Diagnóstico sobre la situación de trata de personas en México", primera edición. CNDH. Tomado de https://www.senado.gob.mx/comisiones/trata_personas/docs/Diagnostico_Trata.pdf 10 de noviembre del 2020

Portal electrónico de la FGR, este *"Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*". Tomado de https://www.

gob.mx/fgr/es/articulos/conoces-el-protocolo-de-palermo?idiom=es#:~:text=Fue%20ratificado%20por%20M%C3%A9xico%20el,contra%20la%20Delincuencia%20Organizada%20Transnacional. 10 de noviembre del 2020

UNODC. "*Diagnóstico Nacional sobre la situación de la Trata de Personas en México*". 2012, obtenido de: https://www.gob.mx/cms/uploads/attachment/file/37682/Diagnostico_UNODC.pdf, 15 de noviembre del 2020

Asociación de Internet MX en su 13° *"Estudio Sobre Hábitos De Los Usuarios De Internet en México"*, tomado de https://irp-cdn.multiscreensite.com/81280eda/files/uploaded/13_Estudio_Habitos_del_Usuario_2017.pdf, 4 de diciembre del 2020

Legisgrafía

Código Penal Federal.

Constitución Política de los Estados Unidos Mexicanos.

Ley general para prevenir, sancionar y erradicar los delitos en materia de trata de personas y para la protección y asistencia a las víctimas de estos delitos.

Programa nacional para prevenir, sancionar y erradicar los delitos en materia de trata de personas y para la protección y asistencia a las víctimas de estos delitos 2014-2018.

Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que contempla la convención de las naciones unidas contra la delincuencia organizada transnacional, adoptado por la asamblea general de las naciones unidas el 15 de noviembre de 2000, 2003, México

CIBERCRIMINALIDAD FINANCIERA: EL PAPEL DE LAS CRIPTOMONEDAS EN EL LAVADO DE DINERO

Silke Mora López*
Héctor Alejandro Ramírez Medina**

"La corrupción, el lavado de dinero y la evasión fiscal, son problemas mundiales, no solo desafíos para los países en desarrollo."
Sri Mulyani Indrawati

SUMARIO: I. Introducción; II. Generalidades del Sistema Financiero Mexicano; III. El funcionamiento de la cripto moneda en el SFM; IV. Dificultades para él rastreo de las operaciones de las criptomonedas; V. Recomendaciones de la GAFI (combate del lavado de dinero) hacia México enfocadas a criptomonedas; VI. Consideraciones finales y recomendaciones; VII. Fuentes de Información.

I. INTRODUCCIÓN

Los cambios en las tecnologías han impactado en la manera de generar dinero en el mundo. Antes era necesario acudir a una sucursal bancaria y ahora, solo basta con darte de alta en línea con los mínimos requisitos para obtener acceso a una plataforma financiera.

Estos mismos cambios han originado que disminuyan los requisitos que antes eran un obstáculo para el público en general. Sin embargo, esa disminución de requisitos ha traído consigo que no siempre sea utilizado de manera adecuada y licita. Si bien, ha traí-

* Licenciada en Derecho y en Contaduría Pública por la UAS, Maestra en Administración de las Contribuciones y Maestra en Derecho por la UNAM. Abogada postulante.

** Economista por la UNAM, académico, columnista y articulista. Jefe de Presupuesto y Coordinador Editorial de la Coordinación del Programa de Posgrado en Derecho. Director General de la Revista Coyuntura Económica. Secretario Académico del Colegio de Economistas Metropolitanos de la CDMX y Miembro de Número de la Asociación de Economistas al Servicio del Estado. Miembro de la Red Nacional de Jóvenes Investigadores del SIJ de la UNAM. Contacto <ale.rmz_medina@hotmail.com> ORCID: <https://orcid.org/0000-0002-0443-3140>.

do enorme beneficio también ha traído aspectos negativos que han impactado en las economías mundiales.[1]

Estas nuevas tecnologías financieras han adaptado sus operaciones para ser útiles a las necesidades de los usuarios que buscan la facilidad para sus incursiones en el sistema financiero. A raíz de ello, surgen las criptomonedas como método de transferencia de dinero a través de códigos encriptados, en donde solo, personas que puedan descodificarlo pueden lograr obtener el dinero que se encuentra valuada en *bitcoins*. Como se ha dicho, este tipo de activo virtual trae consigo diversos aspectos negativos que al sistema financiero mundial no le ha gustado tanto; puesto que cualquier recurso económico puede acceder a esta plataforma sin la necesidad de identificarlo y mover entre la nube a otro país o países en tiempo real, sin que haya sido detectado por alguna autoridad. Lo cual es un problema al momento de saber si, ese dinero es licito o ilícito.

Debido a lo anterior, el presente trabajo abordará los parámetros necesarios que cualquier usuario debe conocer de las criptomonedas en su versión de P2P[2]. En el primer apartado de este trabajo considerará las generalidades del sistema financiero mexicano, puesto que, es necesario ubicar al lector respecto de las tecnologías financieras y el lugar ocupan en nuestro sistema.

En el segundo apartado se abordará el funcionamiento del activo virtual en el Sistema Financiero Mexicano, considerando su evolución en México, así como los desafíos que se ha presentado en nuestro país.

En la tercera parte del presente trabajo se hablará de las dificultades para el rastreo de las operaciones de las criptomonedas en los sistemas financieros internacionales y las consecuencias de la falta de regulación internacional respecto de este nuevo instrumento financiero. Puesto que es altamente riesgos.

1 Critomonedastop,https://criptomonedastop.com/impacto-las-criptomonedas-la-economia-mundial/#:~:text=Son%20operaciones%20mucho%20m%C3%A1s%20flexibles,trabajar%20sobre%20el%20sistema%20financiero, fecha de consulta: 30 de octubre de 2020.

2 Peer-to-peer, red de pares, red entre iguales o red entre pares

Y la última parte se adentrará a las recomendaciones que Grupo de Acción Financiera Internacional (GAFI) ha realizado a México para evitar el lavado de dinero a través de los activos virtuales que se encuentran como criptomoneda, aquí se tratará cual ha sido nuestro cumplimiento como país y cuales han sido nuestras deficiencias respecto a estas recomendaciones.

II. GENERALIDADES DEL SISTEMA FINANCIERO MEXICANO

Empezaremos por definir al sistema financiero como "el conjunto de instituciones, mercados e instrumentos en el que se organiza la actividad financiera, para movilizar el ahorro a sus usos más eficientes."[3]

Por lo anterior podemos entender que el sistema financiero mexicano se refiere a un mercado financiero organizado y se define como el conjunto de instituciones que generan, recogen, administran y dirigen tanto el ahorro como la inversión, dentro de una unidad política-económica, y cuyo establecimiento se rige por la legislación que regula las transacciones de activos financieros y por los mecanismos e instrumentos que permiten la transferencia de esos activos entre ahorrantes, inversionistas o los usuarios del crédito, también puede entenderse como, un grupo de instituciones que se encargan de proporcionar financiamiento profesional a las personas físicas y morales y a las actividades económicas del país, ya que agrupa a diversas instituciones u organismos interrelacionados que se caracterizan por realizar una o varias de las actividades tendientes a la capacitación, administración, regulación, orientación y canalización de los recursos económicos de origen nacional e internacional.

---

3 http://educa.banxico.org.mx/banco_mexico_banca_central/sistema-financiero.html consultado el 10 de noviembre de 2020.

La función del sistema financiero es la creación, intercambio, transferencia y liquidación de activos y pasivos financieros. No es más que una rama económica adicional, que, en vez de producir bienes, produce servicios demandados por la población. El sistema financiero está organizado para recibir dinero de quienes lo tienen en exceso, para negociarlo y transferirlo a quienes carecen de él. Como cualquier mercado donde se intercambian productos y se establecen los precios, el sistema financiero se intercambia dinero y se determina su precio, logrando así equilibrar los recursos monetarios disponibles.

Entre los objetivos del sistema financiero se encuentran, captar los excedentes de efectivo y transfiere los ahorros a los demandantes de dinero, corregir las descompensaciones en el gran flujo económico y finalmente, propiciar el desarrollo y crecimiento de la economía.

El fundamento constitucional lo encontramos en el artículo 28 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) en su párrafo sexto, que a la letra dice, "El Estado tendrá un banco central que será autónomo en el ejercicio de sus funciones y en su administración. Su objetivo prioritario será procurar la estabilidad del poder adquisitivo de la moneda nacional, fortaleciendo con ello la rectoría del desarrollo nacional que corresponde al Estado. Ninguna autoridad podrá ordenar al Banco conceder financiamiento."[4]

Por otra parte, en el séptimo párrafo encontramos que, "no constituye monopolios las funciones que el Estado ejerza de manera exclusiva a través del banco central en las áreas estratégicas de acuñación de monedas y emisión de billetes. El banco central, en los términos que establezca las leyes y con intervención que corresponda a las autoridades competentes, regulará los cambios, así como la intermediación y los servicios financieros, contento con las atribuciones de autoridad necesaria para llevar a cabo dicha regulación y proveer a su observancia…"[5]

4 Constitución Política de los Estados Unidos Mexicanos, Editorial Porrúa, México, 2012

5 Ibid.

El marco jurídico o legislación que ordena el sistema financiero es la siguiente:

- Constitución Política de los Estados Unidos Mexicanos.
- Ley Monetaria
- Ley Orgánica Nacional Financiera
- Ley Orgánica del Banco del Ahorro Nacional y Servicios Financieros
- Ley de Fondos de Inversión
- Ley de la Sociedad Hipotecaria Federal
- Ley de Instituciones de Crédito
- Ley de Protección al Ahorro Bancario
- Ley de los Sistemas de Ahorro Para el Retiro
- Ley de Transparencia y Fomento a la Competencia de Crédito Garantizado
- Ley de Uniones de Crédito
- Ley General de Organizaciones y Actividades Auxiliares del Crédito
- Ley Para Regular las Agrupaciones Financieras
- Ley Para Regular Las Sociedades de Información Crediticia
- Ley del Banco de México
- Ley General de Títulos y Operaciones de Crédito
- Ley Para la Transparencia y Ordenamiento de los Servicios Financieros
- Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI).
- Ley para Regular las Instituciones de Tecnología Financiera
- Ley Nacional de Extinción de Dominio

Dentro del sistema financiero mexicano se encuentran Entidades Reguladoras, Normativas y de Vigilancia, mismas que enunciaremos a continuación junto con una breve descripción de su funcionamiento, a saber,

1. Banco de México

El Banco de México (BANXICO) es el banco central de la República Mexicana y es, como vimos anteriormente, una entidad autónoma del Gobierno Federal. Su finalidad es proveer a la economía del país de moneda nacional y su objetivo prioritario es procurar la estabili-

dad de precios, es decir, mantener la inflación baja, para así preservar el poder adquisitivo de la moneda nacional. Adicionalmente le corresponde promover el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pago.

En materia financiera, el Banco de México puede emitir regulación para fomentar el sano desarrollo del sistema financiero. Una buena parte de las normas emitidas por el BANXICO tiene como propósito regular las operaciones de crédito, de depósito y los servicios que ofrecen los bancos y las casas de bolsa. Recientemente, el Congreso de la Unión le otorgó facultades al Banco de México para que emita regulación sobre comisiones y tasas de interés, así como cualquier otro concepto de cobro por las operaciones o servicios que las entidades financieras lleven a cabo con los clientes.

2. Secretaría de Hacienda y Crédito Público

La Secretaría de Hacienda y Crédito Público es una entidad que forma parte del Gobierno Federal. Regula todo lo relativo a los ingresos del gobierno. El más importante de estos ingresos son los impuestos que las personas y las empresas tienen que pagarle al gobierno para que éste cuente con los recursos suficientes para cumplir con sus funciones. Otra función importante de la Secretaría de Hacienda es establecer el nivel de endeudamiento del gobierno federal, es decir, establecer el límite de deuda que el gobierno puede asumir. También tiene como responsabilidad establecer los gastos (egresos) que el gobierno va a realizar en un determinado periodo. Antes de poder realizar dichos gastos, la secretaría le envía a la Cámara de Diputados del Congreso de la Unión un documento que se conoce como Presupuesto de Egresos, para que la Cámara apruebe los gastos que el gobierno federal espera realizar en un determinado año calendario. En materia financiera y bancaria, la Secretaría de Hacienda es la encargada de planear, coordinar, evaluar y vigilar el sistema bancario del país. Entre sus facultades, está emitir normas para regular a las oficinas de representación y las filiales de entidades financieras

del exterior, y expedir los reglamentos orgánicos de los bancos de desarrollo.

3. Comisión Nacional Bancaria y de Valores

La Comisión Nacional Bancaria y de Valores (CNBV) es un organismo que forma parte del Gobierno Federal y que tiene como funciones vigilar (supervisar) y regular a las entidades que forman parte del sistema financiero mexicano para lograr su estabilidad, buen funcionamiento y sano desarrollo. Asimismo, es la autoridad encargada de autorizar a los intermediarios que deseen ingresar al mercado financiero. Las entidades que regula la CNBV y que forman parte del sistema financiero son los bancos (instituciones de crédito), las casas de bolsa, las sociedades de inversión, las sociedades financieras de objeto limitado (sofoles), las sociedades financieras de objeto múltiple (sofomes), las arrendadoras financieras, las empresas de factoraje financiero, las sociedades financieras populares (sofipos) y las sociedades cooperativas de ahorro y préstamo. La CNBV tiene la facultad de emitir regulación prudencial cuyo propósito es limitar los incentivos a tomar riesgos. Es decir, esta regulación prudencial busca limitar la toma excesiva de riesgos por parte de los intermediarios para evitar que realicen operaciones que puedan provocar su falta de liquidez o solvencia.

4. Comisión Nacional de Sistemas de Ahorro para el Retiro

La labor de la Comisión Nacional del Sistema de Ahorro para el Retiro es regular al Sistema de Ahorro para el Retiro (SAR). El SAR engloba todas las aportaciones que hacen los trabajadores y las empresas, durante la vida laboral de los trabajadores, a una cuenta de ahorro cuyo dueño (titular) es cada uno de los trabajadores (cuentas individuales). Dichas cuentas individuales sirven para que los trabajadores, una vez que alcancen su edad de retiro (como jubilados o pensionados), tengan los recursos suficientes para poder cubrir sus gastos y como previsión social. La Consar establece las reglas para que el SAR funcione adecuadamente.

La Consar también regula a las empresas administradoras de fondos para el retiro (afores), que son las empresas que administran estas cuentas individuales de los trabajadores, ya que la Consar también vigila que se resguarden de manera adecuada los recursos de los trabajadores.

5. Comisión de Defensa de los Usuarios de Servicios Financieros

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros es la entidad encargada de informar, orientar y promover la educación financiera entre la población, así como atender y resolver las quejas y reclamaciones de los clientes en contra de cualquier banco.

6. Unidad de Inteligencia Financiera

Es la instancia central nacional para recibir reportes de operaciones financieras y avisos de quienes realizan actividades vulnerables; analizar las operaciones financieras y económicas y otra información relacionada; y, diseminar reportes de inteligencia y otros documentos útiles para detectar operaciones probablemente vinculadas con el lavado de dinero (LD) o el financiamiento al terrorismo (FT), y en su caso, presentar las denuncias correspondientes ante la autoridad competente.

Las principales tareas de la Unidad de Inteligencia Financiera consisten en implementar y dar seguimiento a mecanismos de prevención y detección de actos, omisiones u operaciones, que pudieran favorecer, prestar ayuda, auxilio o cooperación de cualquier especie para la comisión de los delitos previstos en los artículos 139 y 140 del Código Penal Federal.

7. Intermediarios Financieros

Los intermediarios financieros son las instituciones que obtienen su capital a través de un prestamista y los pone a disposición de los prestatarios. Ejemplo de su actividad es la actividad de la Banca

Comercial, que utiliza el dinero de sus clientes en cuentas de ahorro para después prestarlo a terceros (ya sea individuos, empresas o el mismo gobierno) y así obtener ganancias a través de intereses.

8. Organismos de apoyo

Son aquellas empresas que no están autorizadas a recibir y utilizar grandes cantidades de efectivo del público ni recibir depósitos en cuenta de cheques, es decir sólo complementan los servicios bancarios.

En ese sentido, podemos entender que el Sistema Financiero Mexicano se encuentra supervisado, regulado y normado por entidades diversas que generan confianza y certeza en la naturaleza lícita de las operaciones y transacciones que se llevan día a día.

III. EL FUNCIONAMIENTO DE LA CRIPTO MONEDA EN EL SISTEMA FINANCIERO MEXICANO

La criptomoneda aparece en el sistema financiero internacional a partir de 2009 a través de *Bitcoin*, ha revolucionado los mercados financieros regulados:

> *"La primera criptomoneda que surgió en el mundo se conoce como Bitcoin; esto ocurrió cuando una entidad en anonimato, en un sistema electrónico abierto al pulico, predefinió un esquema de pago con esa criptomoneda, estableciendo la forma de su creación, la forma de llevar a cabo transacciones con el, así como todos los protocoles necesarios para dar seguridad a este esquema de pagos. Después de la Bitcoin han surgido muchas otras criptomonedas, por ejemplo, Ethereum y Ripple; aunque sus orígenes pueden ser distintos, cada una de ellas está representada por un registro digital basado en código encriptados; adicionalmente, tienen sus propios protocoles y reglas de uso."* [6]

Se observa que las Normas de Información Financiera le da la calidad de criptomonedas, pero lo cierto es que, son activos vir-

6 C-22 Criptomonedas, Normas de Información Financieras

tuales conforme a la regulación que existe en México, lo cual será abordado más adelante. Es importante hacer notar esto, porque puede confundirse la criptomoneda como una moneda avalada y en curso legal, cuando esto no es así.

En virtud de que, el valor de un activo a transmutado a expresiones matemáticas e informáticas, es decir, activos impalpables que son valuados en dinero y que pueden ser objeto de comercio entre particulares.

Su creado es Satoshi Nakamoto, el cual, menciona que la criptomoneda es una moneda electrónica que se basa en una cadena de firmas digitales.[7] El creador de esta moneda le da la naturaleza de moneda. Esta moneda no es regulada en muchos países, y tiene la calidad de activo virtual. Por ejemplo, en México existe la Ley Monetaria de los Estados Unidos Mexicanos, la cual regula y señal que nuestra moneda es el peso y que las únicas monedas circulantes en territorio nacional son:

- Los billetes del Banco de México, S.A.
- Las monedas metálicas de denominaciones específicas señaladas en la propia ley.
- Las monedas metálicas conmemorativas de acontecimientos de importancia nacional.[8]

Asimismo, el artículo 8 de la Ley Monetaria de los Estados Unidos Mexicanos, que la moneda extranjera no tendrá curso legal en la República. Y en el caso de cumplimiento de obligaciones en moneda extranjera contraídas dentro o fuera de la República para ser cumplidas en ésta, se solventarán entregando el equivalente en moneda nacional, al tipo de cambio que rija en el lugar y fecha en que se haga el pago. De tal forma que, en México no es considera una moneda, pero si un activo que puede valuarse en dinero.

---

7 Sánchez Roa, Julia. Criptomonedas. Página web: https://www.pj.gob.py/ebook/monografia s/extranjero/civil/Julia-Sanchez-Criptomonedas.pdf, fecha de consulta: 30 de octubre de 2020.

8 Artículo 2 de la Ley Monetaria de los Estados Unidos Mexicanos

En este contexto, puede afirmarse que, una criptomoneda puede definirse como una divisa digital o virtual que usa criptografía para su seguridad y no está emitida por ninguna autoridad central, lo cual la deja prácticamente inmune a interferencias o manipulaciones de los gobiernos. [9]

Sin embargo, el catalogar a un activo virtual (ejemplo Bitcoin) como divisa digital, se estaría cayendo en un error; si bien, puede existir un intercambio de esta por algún tipo de acto o servicio, lo cierto es que, las divisas solo operan con un valor monetario regulado, y este activo, le da un valor contralado por agentes diversos a una institución financiera. Lo que si puede decirse es que operan de manera similar a un mercado de divisas, situación que es totalmente diferente. Entonces, al no ser emitidas o respaldadas por un gobierno extranjero, tampoco pueden ser consideradas divisas.

El Banco Central Europeo señala la *virtual currency* es la representación digital de valor, no emitida por ninguna autoridad central, institución de crédito o emisor de dinero electrónico reconocido que, en ciertas ocasiones, puede ser utilizada como medio de pago alternativo de dinero.[10]

Definición que resulta más acertada. Como se dijo al inicio de este apartado, los activos virtuales nacen de la criptografía en donde a través de ecuación matemáticas va llegando a la liberación del valor y con ello, llegue a su destino final. Esto solo se encontrará de manera digital, no puede representarse en el mundo terrenal, hasta que este sea convertido a una moneda en curso de algún país, lo que significa que se encuentra dentro de una institución financiera.

Entonces, el activo virtual debe basarse en códigos encriptados, pero su finalidad es utilizarlos como medio de pago, de no ser así

---

9 Sánchez Roa, Julia. Criptomonedas. Página web: https://www.pj.gob.py/ebook/monografias/extranjero/civil/Julia-Sanchez-Criptomonedas.pdf, fecha de consulta: 30 de octubre de 2020.

10 Banco Central Europeo. Virtual currency schemes – a further analysis. Página web: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf p.13, fecha de consulta: 30 de octubre de 2020.

solo tendría la calidad de un criptoactivo[11]. Los criptoactivos puede ser de dos formas: tokens y activos virtuales(criptomoneda). Las formas de obtención de este activo virtual, puede ser a través de la minería, plataformas digitales de intercambio:

> *"…compensación de mineros a los mineros por actividades de minería; el lanzamiento de ofertas iniciales de criptomonedas (Initial Coin Offering, ICO) hacia el público en general o hacia un mercado especifico; o bien, la colación de un cierto número de criptomonedas dentro de un sistema activo o mercado cautivo sin costo para los usuarios. Posteriormente, las criptomonedas son negociadas o utilizadas como medio de pago en la medida en que son aceptadas por los participantes del mercado. Es a través de las plataformas digitales de intercambio (exchanges) que se llevan a cabo la compra, venta y, en general, las transferencias de criptomoneda; a menudo también se utilizan los monederos de criptomoneda (wallets) que permiten su almacenamiento y transferencia…"*[12]

Al respecto, los contratos por diferencia (la obtención a través del comercio) son productos apalancados que permiten abrir una posición con tan solo una fracción del valor total de la operación. Es decir, hace referencia a la especulación sobre si el mercado elegido aumentará o disminuirá en valor[13]. En cuanto a los mineros (minado) son quienes aportan la seguridad a las transacciones utilizando, en la mayor parte de los casos, la tecnología de blockchain (cadena de bloques).

Una vez discutido esto, en cierto país se encuentra altamente regulado, tal es el caso de España. Sin embargo, el presente estudio se hará enfocándose en la situación de México.

Bien, este activo virtual se encuentra regulado en México a partir del 2018, con la publicación en el Diario Oficial de la Federación de la Ley para Regular las Instituciones de Tecnología Financiera; esta Ley tiene por objeto regular los servicios financieros que pres-

---

11 C-22 Criptomonedas, Normas de Información Financieras

12 C-22 Criptomoneda, Normas de Información Financiera

13 Ricou, Eduardo. Página web: https://libertex.org/es/blog/que-son-las-criptomonedas-y-como-funcionan fecha de consulta: 31 de octubre de 2020.

tan las instituciones de tecnología financiera, así como su organización, operación y funcionamiento y los servicios financieros sujetos a alguna normatividad especial que sean ofrecidos o realizados por medios innovadores.[14]

El capítulo III denominado "De las operaciones con activos virtuales" existe un apartado especial para los activos virtuales (criptomonedas), en donde señala que:

> *"la representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional, las divisas ni cualquier otro activo denominado en moneda de curso legal o en divisas."* [15]

De lo anterior puede desprenderse las características de un activo virtual: 1) No es considerada moneda en territorio nacional, 2) es un registro electrónico que tiene un valor valuable en dinero, 3) es un medio de pago para cualquier acto o actividad licita, 4) solo existe en una nube a través de medios electrónicos.

Si bien a lo largo del presente apartado se ha abordado que los activos virtuales no son moneda en curso, la ley en comento señala que pueden ser utilizadas como medio de pago; sin embargo, el hecho de que una criptomoneda pueda ser utilizada como un medio de pago, no las hace monedas para efectos legales mexicanos, tal y como fue abordado anteriormente, aun y cuando estas Instituciones Tecnológicas Financieras se encuentren bajo autorización del Banco de México, ya que, solo se está autorizando la estructura corporativa de estas instituciones pero no del activo virtual, puesto que no es respaldado por ninguna institución financiera en el mundo.

---

14 Artículo 1 de la Ley para Regular las Instituciones de Tecnología Financiera

15 Artículo 30 de la Ley para Regular las Instituciones de Tecnología Financiera

Por el hecho ser un activo muy volátil y no encontrarse respaldado por alguna institución financiera, trae consigo que pueda introducirse dinero de actividades ilícitas sin ser observadas o auditadas por alguna autoridad:

> *"En distintos foros, las autoridades financieras, nacionales e internacionales, han advertido sobre los riesgos de invertir en criptomonedas, dado que típicamente no tiene respaldo económico por parte de los bancos centrales, de la banca comercial o del gobierno. Comúnmente tiene una alta volatibilidad por tener una alta actividad especulativas; no obstante, en el entorno económico actual, nacional e internacional, se lleva a cabo una gran cantidad de transacciones con este tipo de activos."* [16]

Siguiendo el contexto internacional, la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, incluyó como actividad vulnerable dentro de su artículo 17, a los activos virtuales:

> *El ofrecimiento habitual y profesional de intercambio de activos virtuales por parte de sujetos distintos a las Entidades Financieras, que se lleven a cabo a través de plataformas electrónicas, digitales o similares, que administren u operen, facilitando o realizando operaciones de compra o venta de dichos activos propiedad de sus clientes o bien, provean medios para custodiar, almacenar, o transferir activos virtuales distintos a los reconocidos por el Banco de México en términos de la Ley para Regular las Instituciones de Tecnología Financiera. Se entenderá como activo virtual toda representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional, las divisas ni cualquier otro activo denominado en moneda de curso legal o divisas.* [17]

Lo anterior, debido a que el activo virtual en comento al no encontrarse respaldado por alguna institución financiera, no se tiene conocimiento quien recibe y quien emite. Si no hasta que alguno de ellos, incorpora el dinero en el sector financiero y es localizado

16 C-22 Criptomoneda, Normas de Información Financiera.

17 Artículo 17 de la LFPIORPI

o identificado por la autoridad financiera y en su caso la autoridad hacendaria.

Esto debido a los altos estándares de seguridad desarrollados en el activo virtual, ninguna autoridad o tercero podrá tener información de las cuentas que existen en la nube y mucho menos conocer de donde salió o entro el dinero. Lo cual será abordado en el siguiente apartado.

IV. DIFICULTADES PARA ÉL RASTREO DE LAS OPERACIONES DE LAS CRIPTOMONEDAS

La nueva movilidad del dinero y su valuación atravesó fronteras; ahora, podemos adquirir y enviar en cuestión de minutos a otra persona y si bien, esta parte ya existía, lo que no formaba parte de nuestro entorno económico es que se pudiera enviar y producir dinero a través de una nube electrónica; y que él envió o ganancia (minado) de ese dinero estaría en completo anonimato. Como fue comentado en el apartado anterior, este tipo de activo es utilizado por cualquier persona, sin embargo, también puede trasladar dinero de obtención ilícita por la no de identificación de usuarios y del dinero que ahí se encuentra.

Este nuevo reto para todas las autoridades, principalmente a la Hacendaria se enfrenta a una economía y formas de transacción que van evolucionando con rapidez y a esta se le dificulta poder alcanzar la realidad.

El aspecto tributario ha sido rebasado y debe implementarse nuevos mecanismos para la detección del ingreso, tanto para aspectos de impuesto, pero también de origen del dinero; esto, con la finalidad de ir disminuyendo su operación por actividades ilícitas.

Se ha mencionado que este tipo de activo virtual pide los mínimos de identificación para que cualquier usuario pueda operar en él, si bien es cierto que algunas empresas solicitan identificación de los usuarios para un tránsito más elevado de criptomonedas, esto no

da una certeza si en realidad esta persona es quien lleva a cabo las operaciones, así como el origen y destino de dicho recurso económico; puesto que no hay que olvidar que una característica de este instrumento financiero es que las empresas que administran, vigilar y salvaguardan este tipo de activo virtual otorgan un anonimato a las personas que en ellas se encuentran:

> *Por tanto, el anonimato en el sistema Bitcoin radica en la imposibilidad de vincular cualquier clave pública con su usuario. Tan sólo podría llegar a conocerse la identidad del interviniente de la operación Bitcoin si, de alguna manera, se identifica a un determinado sujeto con una dirección o clave pública Bitcoin, en este caso resultaría sencillo rastrear en la blockchain todas las operaciones realizadas por este sujeto (es la situación que viene a denominarse loss of transactional privacy)* [18]

En esta tesitura, el anonimato en este activo virtual se refuerza con la desvinculación o *unlinkability* del seudónimo utilizado para realizar transacciones con este activo virtual. Por lo que, el usuario al no desvincularlo lo que ocurre es que puede ubicarse el usuario, esto a través del IP del dispositivo tecnológico que utilice; por lo que, el anonimato no es absoluto, sino relativo:

> *"Como hemos expuesto, la seudonimia no asegura per se el anonimato de los usuarios, ya que es posible, en algunos casos, establecer una relación entre la clave pública o dirección de Bitcoin y la identidad real del usuario. No obstante, el anonimato puede llegar a alcanzarse si a la seudonimia se une la propiedad de desvinculación (unlinkability) del sistema.* "[19]

Algunos ejemplos de esto son: el uso de software que mezcla múltiples direcciones de Bitcoins para dificultar o imposibilitar el rastreo del usuario que realizó la operación sujeta a gravamen, o el cambio de Bitcoins por otras criptodivisas que permiten un anoni-

---

18 Pérez Bernabeu, Begoña. La Administración tributaria frente al anonimato de las criptomonedas: la seudonimia del Bitcoin. VI Encuentro de Derecho Financiero y Tributario. 2018. España.

19 Ibidem

mato absoluto.[20]

En el fondo, se persigue proteger el anonimato de un usuario de Bitcoin del resto de usuarios del sistema. Gracias a la tecnología blockchain, antes descrita, la unlinkabilityes posible. En el sistema del activo virtual, es posible hablar de «trazabilidad» de las operaciones al quedar almacenadas en blockchain, pero se conserva el anonimato de los intervinientes en las distintas transacciones debido a la utilización de claves públicas o direcciones (que hacen las funciones de seudónimo.[21]

En una investigación, las autoridades deberán obtener información acerca de las protecciones que cada cuenta tiene acerca de sus datos informáticos y si, a raíz de ellos puede obtenerse información suficiente y necesaria para vincular algún proceso penal o fiscal, en su caso.

V. RECOMENDACIONES DE LA GAFI (COMBATE DEL LAVADO DE DINERO) HACIA MÉXICO ENFOCADAS A CRIPTOMONEDAS

Es conocido que la recomendación 15 del Grupo de Acción Financiera Internacional (GAFI) enfocada a las nuevas tecnologías dice que,

> *"Los países y las instituciones financieras deben identificar y evaluar los riesgos de lavado de activos o financiamiento del terrorismo que pudieran surgir con respecto a (a) el desarrollo de nuevos productos y nuevas prácticas comerciales, incluyendo nuevos mecanismos de envío, y (b) el uso de nuevas tecnologías o tecnologías en desarrollo para productos tanto nuevos como los existentes. En el caso de las instituciones financieras, esta evaluación del riesgo debe hacerse antes del lanzamiento de los nuevos productos, prácticas comerciales o el uso de tecnologías nuevas o en desarrollo. Los países y las instituciones financieras deben tomar medidas apropiadas para administrar y mitigar esos riesgos."*[22]

20 Ibidem

21 Ibidem

22 Gafi, Estándares Internacionales Sobre La Lucha Contra El Lavado De Activos,

Desde 2014 en BANXICO en un comunicado de prensa de 10 de marzo emitió una serie de advertencias acerca del uso de activos virtuales entre los que encontramos, que no son monedas de curso legal ni en México ni en el mundo al no estar respaldada, regulada ni supervisada por ninguna autoridad monetaria nacional o internacional, lo anterior no les permite cumplir con la función de medio de pago que libere de alguna obligación en el SFM, ya que las instituciones que lo componen no están autorizadas a efectuar operaciones con ellas.[23]

En la Primera Evaluación Nacional de Riesgos (ENR) de Lavado de Dinero y Financiamiento al Terrorismo en México, la cual fue interinstitucional[24] se reconocía que el diseño de los avisos y modelos de alerta y descripción de los Sujetos Obligados de reportar Actividades Vulnerables no cumplía al 100% las recomendaciones del GAFI.[25]Tambien reconocía los altos riesgos de muchas de las instituciones financieras no reguladas como SOFOMES, Sociedades Operadoras de Sociedades de Inversión, Transmisores de Dinero y Asesores en inversión.[26]

El Financiamiento Del Terrorismo Y De La Proliferación, 2012. Encuéntrese en https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Spanish.pdf, Fecha de consulta: 15 de octubre de 2020.

23 Véase. Banco de México, Advertencias sobre el uso de activos virtuales como sucedáneos de los medios de pago en moneda de curso legal, Comunicado de Prensa 10 de marzo de 2014 en https://www.banxico.org.mx/publicaciones-y-prensa/miscelaneos/%7B881612EF-DEC3-E03E-8C5A-C795CA66ACEA%7D.pdf consultado el 11 de noviembre de 2020.

24 En la elaboración de la encuesta y construcción de la metodología participaron entre otras, la Secretaría de Gobernación, la Secretaria de Hacienda y Crédito Público mediante la Unidad de Inteligencia Financiera, la entonces Procuraduría General de la República, el Banco de México y el Poder Judicial de la Federación.

25 SHCP, BANXICO, PGR, PJF, SEGOB, Primera Evaluación Nacional de Riesgos (ENR) de Lavado de Dinero y Financiamiento al Terrorismo en México, México 2016, Pág. 31.

26 Ibidem, pág 34.

Para 2017 las autoridades financieras[27] emiten un comunicado de prensa conjunto una alerta que califican de preventiva[28] sobre los riesgos asociados al uso de activos virtuales reiterando que no son moneda de curso legal ni divisas; así mismo destacan que en el uso respectivo de sus atribuciones buscan mantener actualizada la normatividad en función destacando que se en ese momento ya se encontraba en el Congreso de la Unión la discusión del proyecto de Ley para Regular las Instituciones de Tecnología Financiera (Ley Fintech).

En enero de 2018 se dieron a conocer los resultados de la última evaluación mutua a México, esta vez practicada por el Fondo Monetario Internacional, se manifiesta que nuestro país tiene un buen sistema contra el lavado de activos, pero debe ser más consistente en la confiscación de bienes provenientes de actividades ilícitas.[29]En esa evaluación las recomendaciones donde se obtuvo como parcialmente cumplido son las 8, 10, 12, 15, 16, 17, 18, 20, 22, 24, 28,32, 33, 37 y 38.[30]

En su reunión plenaria de 2018 el GAFI emitió una actualización de su recomendación 15, la cual es dirigida a las nuevas tecnologías, en ese sentido reconoció que el uso de activos virtuales o criptomonedas se ha convertido en una gran fuente de realizar el

---

27 Secretaria de Hacienda y Crédito Público, Banco de México y Comisión Nacional Bancaria y de Valores

28 Véase. SHCP - BANXICO – CNVB, Las autoridades financieras advierten de los riesgos asociados al uso de activos virtuales y a la participación en los esquemas de inversión conocidos como Oferta Inicial de Monedas o Initial Coin Offerings, Comunicado de Prensa conjunto 13 de diciembre de 2017 en https://www.banxico.org.mx/publicaciones-y-prensa/miscelaneos/%7B-6D5AAB8C-3BFA-0A8B-5EDD-7EDC04E1931C%7D.pdf, fecha de consulta: 18 de octubre de 2020.

29 Garay Garzón, Víctor Manuel, Mexico: su lucha contra el lavado de activos y su impacto laboral, en Revista de la Facultad de Derecho de México, Tomo LXIX, Número 273, Enero – Abril 2019.

30 GAFI, Medidas antilavado contra la financiación al terrorismo, México, Informe de Evaluación Mutua, Enero de 2018.

lavado de dinero con recursos de procedencia ilícita.[31]

En ese sentido, en México, la Unidad de Inteligencia Financiera de la Secretaria de Hacienda y Crédito Público emitió el 14 de julio pasado los Lineamientos para la Elaboración del Informe de Retroalimentación a los Proveedores de Servicios de Activos Virtuales (VASP)[32] basadas en la recomendación 34 del GAFI *Guía y Recomendación,* y la entrada en vigor de la adhesión de la fracción XVI al artículo 17 de la LFPIORPI[33] que dice,

> *"El ofrecimiento habitual y profesional de intercambio de activos virtuales por parte de sujetos distintos a las Entidades Financieras, que se lleven a cabo a través de plataformas electrónicas, digitales o similares, que administren u operen, facilitando o realizando operaciones de compra o venta de dichos activos propiedad de sus clientes o bien, provean medios para custodiar, almacenar, o transferir activos virtuales distintos a los reconocidos por el Banco de México en términos de la Ley para Regular las Instituciones de Tecnología Financiera. Se entenderá como activo virtual toda representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional, las divisas ni cualquier otro activo denominado en moneda de curso legal o divisas.*
>
> *Serán objeto de Aviso ante la Secretaría cuando el monto de la operación de compra o venta que realice cada cliente de quien realice la actividad vulnerable a que se refiere esta fracción sea por una cantidad igual o superior al equivalente a seiscientas cuarenta y cinco Unidades de Medida y Actualización.*
>
> *En el evento de que el Banco de México reconozca en términos de la Ley para Regular las Instituciones de Tecnología Financiera activos virtuales, las personas*

31 Gutiérrez, Fernando, GAFI pide medidas urgentes para evitar lavado en criptoactivos, El Economista, 22 de octubre de 2018 en https://www.eleconomista.com.mx/economia/GAFI-pide-medidas-urgentes-para-evitar-lavado-en-criptoactivos-20181022-0108.html, revisado el 10 de noviembre de 2020

32 Véase https://www.pld.hacienda.gob.mx/work/models/PLD/documentos/Lineamientos_VASP.pdf

33 Entrada en vigor el 10 de septiembre de 2019, conforme a la Disposición Transitoria Única del Decreto Publicado en el Diario Oficial de la Federación el 09 de marzo del 2018, en el que también se crea la Ley Fintech.

que provean los medios a que se refiere esta fracción, deberán obtener las autorizaciones correspondientes en los plazos que señale dicho Banco de México en las disposiciones respectivas."[34]

Asimismo, también la UIF publicó en 2020 la ENR 2019 -2020 detectó como riesgos emergentes la evolución e innovación tecnológica de las Instituciones de Tecnología Financiera proveedoras de servicios con Activos Virtuales, al ser un sector joven y poca o nula regulación a nivel nacional, internacional o supranacional.[35]

Recientemente, en noviembre de 2020, el Senado de la República aprobó una reforma a la Ley de las Instituciones de Crédito en la que otorga a la UIF de la SHCP poder y facultades legales para bloquear cuentas bancarias sin mediar la orden de un juez, pero que también para garantizar el derecho de audiencia a personas que realizan operaciones con recursos de procedencia ilícita.[36]

VI. CONSIDERACIONES FINALES Y RECOMENDACIONES

Como hemos revisado en el presente análisis, a pesar de las recientes reformas que se han dado para fortalecer al SFM, han sido insuficientes en el combate a la corrupción, la evasión fiscal y el lavado de dinero, puesto que el propio sistema financiero tiene deficiencias entre las que se encuentran la penetración y profundización financiera es bastante baja entre la población mexicana.

Sin lugar a duda quedan reformas pendientes por hacer, entre las que quizá podamos llegar a ver una Unidad de Inteligencia Financiera de la SHCP con facultades ministeriales que nos ayuden a

---

34 Véase http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPIORPI_090318.pdf

35 UIF, Evaluación Nacional de Riesgos de Lavado de Dinero y Financiamiento al Terrorismo en México 2019-2020, México 2020, Pág. 24 y 25

36 Moreno, Teresa; Aprueba Senado a UIF bloquear cuentas bancarias sin permiso de un juez, EL UNIVERSAL, 18 de noviembre de 2020 encuéntrese en https://www.eluniversal.com.mx/nacion/los-senadores-aprueban-reforma-para-fortalecer-la-uif-de-santiago-nieto

que la reforma de noviembre de 2020 sea más garantista del debido proceso y del Estado de Derecho.

Por supuesto, faltan reformas que nos permitan cubrir por completo las recomendaciones que en la Evaluación de 2018 se obtuvo calificación de Parcialmente Cumplido (PC) y que tienen que ver con la transacción de activos virtuales como son mayor regulación a las Organizaciones sin Fines de Lucro (recomendación 8 y que ya se encuentra en propuesta de reforma), las transferencias electrónicas deberán tener mejor rastreo (recomendación 16), seguir mejorando el recientemente reformado reporte de operaciones sospechosas (recomendación 20) y la transparencia y beneficiario final de las personas jurídicas (recomendación 24), y la asistencia legal mutua (recomendaciones 37 y 38).

Se deberá buscar la mayor interacción entre el Sistema de Administración Tributaria, con sus reformas debidas, y la propia Unidad de Inteligencia Financiera, junto con la Comisión Nacional Bancaria y de Valores, para terminar de amalgamar ese trípode anticorrupción operaciones con fines de procedencia ilícita.

Por último, proponemos una reforma a la Ley Fintech que recomiende al BANXICO mejorar el sistema de pagos a fin de que se detecten con mayor facilidad este tipo de operaciones no reconocidas, así como terminar de armonizar la Ley Nacional de Extinción de Dominio.

VII. FUENTES DE INFORMACIÓN.

Libros

Pérez Bernabeu, Begoña. La Administración tributaria frente al anonimato de las criptomonedas: la seudonimia del Bitcoin. VI Encuentro de Derecho Financiero y Tributario. 2018. España.

Hemerografía

Garay Garzón, Víctor Manuel, México: su lucha contra el lavado de activos y su impacto laboral, en Revista de la Facultad de Derecho de

México, Tomo LXIX, Número 273, Enero – Abril 2019.

UIF, Lineamientos para la Elaboración del Informe de Retroalimentación a los Proveedores de Servicios de Activos Virtuales (VASP), México 2020.

GAFI, Medidas antilavado contra la financiación al terrorismo, México, Informe de Evaluación Mutua, Enero de 2018.

UIF, Evaluación Nacional de Riesgos de Lavado de Dinero y Financiamiento al Terrorismo en México 2019-2020, México 2020

GAFI, Estándares Internacionales Sobre La Lucha Contra El Lavado De Activos, El Financiamiento Del Terrorismo Y De La Proliferación, 2012

SHCP, BANXICO, PGR, PJF, SEGOB, Primera Evaluación Nacional de Riesgos (ENR) de Lavado de Dinero y Financiamiento al Terrorismo en México, México 2016.

Fuentes electronicas

Banxico Educa – Sistema Financiero en http://educa.banxico.org.mx/banco_mexico_banca_central/sistema-financiero.html

Gutiérrez, Fernando, GAFI pide medidas urgentes para evitar lavado en criptoactivos, El Economista, 22 de octubre de 2018 en https://www.eleconomista.com.mx/economia/GAFI-pide-medidas-urgentes-para-evitar-lavado-en-criptoactivos-20181022-0108.html

Banco de México. Advertencias sobre el uso de activos virtuales como sucedáneos de los medios de pago en moneda de curso legal. Comunicado de Prensa del 10 de marzo de 2014 en https://www.banxico.org.mx/publicaciones-y-prensa/miscelaneos/%7B881612EF-DEC3-E03E-8C5A-C795CA66ACEA%7D.pdf

SHCP - BANXICO – CNVB, Las autoridades financieras advierten de los riesgos asociados al uso de activos virtuales y a la participación en los esquemas de inversión conocidos como Oferta Inicial de Monedas o “Initial Coin Offerings”, Comunicado

de Prensa conjunto 13 de diciembre de 2017 en https://www.banxico.org.mx/publicaciones-y-prensa/miscelaneos/%7B-6D5AAB8C-3BFA-0A8B-5EDD-7EDC04E1931C%7D.pdf

Ricou, Eduardo. Página web: https://libertex.org/es/blog/que-son-las-criptomonedas-y-como-funcionan

Sánchez Roa, Julia. Criptomonedas. Página web: https://www.pj.gob.py/ebook/monografias/extranjero/civil/Julia-Sanchez-Criptomonedas.pdf

BCE. Virtual currency schemes – a further analysis. Página web: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

Critomonedastop, https://criptomonedastop.com/impacto-las-criptomonedas-la-economia-mundial/#:~:text=Son%20operaciones%20mucho%20m%C3%A1s%20flexibles,trabajar%20sobre%20el%20sistema%20financiero

Moreno, Teresa; Aprueba Senado a UIF bloquear cuentas bancarias sin permiso de un juez, EL UNIVERSAL, 18 de noviembre de 2020 encuéntrese en https://www.eluniversal.com.mx/nacion/los-senadores-aprueban-reforma-para-fortalecer-la-uif-de-santiago-nieto

Legisgrafía

Constitución Política de los Estados Unidos Mexicanos

Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita.

Ley para Regular las Instituciones de Tecnología Financiera.

Ley Monetaria de los Estados Unidos Mexicanos

Normas de Información Financiera

LA FRAGMENTACIÓN DE LA DELINCUENCIA ORGANIZADA Y SU RELACIÓN CON LA VIOLENCIA EN EL CONTEXTO DEL COVID-19 EN MÉXICO

Magdalena Alcocer Vega*
Mariana Lucía Pérez Pérez**

SUMARIO: I. Introducción. II. Conceptualizando a la Delincuencia Organizada. III. Conceptualizando el término de fragmentación. IV. Las causas de fragmentación en nuestro país y su materialización en violencia. V. La agenda presidencial de seguridad en México. VI. Contexto actual de la Delincuencia Organizada en el marco de la emergencia sanitaria por COVID-19 VII. Conclusiones. VIII. Fuentes de consulta.

I. INTRODUCCIÓN

El estudio de la delincuencia organizada en México ha cobrado gran relevancia durante las últimas décadas, por ser considerada una amenaza evolutiva y generadora de altos índices de violencia. Al analizar el fenómeno específico de la fragmentación dentro de las dinámicas de la delincuencia organizada, se pretende conocer si existe una relación causal entre ésta y el aumento de la violencia en el país, a pesar de encontrarse inmerso en el contexto de la pandemia del COVID-19. La delincuencia organizada se caracteriza por contar con un alto grado de adaptabilidad, por lo que la pandemia del COVID-19 únicamente provocó cambios en sus dinámicas, mas no la extinguió.

Durante el 2020 las amenazas asimétricas a la seguridad nacional fueron una constante. El mundo mostró que la certidumbre en

*Coordinadora de la Carrera de Inteligencia Estratégica de la Universidad Anáhuac Campus Norte
** Estudiante de la Licenciatura en Inteligencia Estratégica de la Universidad Anáhuac Campus Norte

materia de seguridad se volvió un objetivo aún más complejo. Si bien, la delincuencia organizada ha estado presente desde hace décadas en las Agendas de Riesgos, a partir del 2020 las amenazas en materia de salud también serán una constante.

Incluso, algunos países ya habían logrado prospectar un acercamiento a la pandemia del COVID-19. En el 2000 surgió un reporte de la Agencia Central de Inteligencia de los EEUU (CIA) titulado "*The Global Infectious Disease Threat and Its Implications for the United States*" que concluía que surgirían infecciones que representarían una amenaza de salud mundial que complicaría la seguridad de los Estados Unidos en los próximos 20 años.[1] Por su parte, la Estrategia de Seguridad Nacional del Reino Unido en 2008, citaba a las pandemias como uno de los riesgos diversos, pero como un paquete de amenazas interconectadas que lo afectarían directamente y que tendrían el potencial de reducir en buena medida la estabilidad internacional".[2]

El informe de 2008 titulado *"Global Trends"* predijo como ningún otro, el surgimiento de una pandemia global; sin embargo, lo ubicaba temporalmente hacia el año 2025 en el sudeste de Asia y derivado de los virus de influenza como el coronavirus.[3] Lo que se veía tan lejano desde occidente en otras latitudes con relación a las pandemias, se hizo realidad y la pandemia puso sobre la mesa las vulnerabilidades en casi todo el espectro de políticas públicas dejando una crisis sin precedentes a nivel económico, político, social y en un impase a los estados en materia de seguridad.

Aunado a lo anterior, las dinámicas de la fragmentación de los grupos delincuenciales continuaron presentándose durante el 2020, por lo que su análisis resulta de gran importancia.

---

1 Le Gloannec, Anne-Marie, Irondelle, Bastien, and Cadier, David, eds. (2013), "New and Evolving Trends in International Security", Transworld Working Papers, No.13 (April), p.10, véase http://www.transworld-fp7.eu/?p=1175

2 Ibidem

3 Global Trends 2025: A transformed World, Office of the Director of National Intelligence, 2008, p. 75 véase https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2025_Global_Trends_Final_Report.pdf

En el siguiente texto se definirá el concepto de Delincuencia Organizada y sus antecedentes en México, para después conocer qué es la fragmentación y algunos factores que facilitaron dicho fenómeno. Posteriormente se describirá cómo la fragmentación se ha materializado en violencia y finalmente se definirán los esfuerzos realizados en materia de seguridad por parte de la administración del presidente Andrés Manuel López Obrador. Cabe mencionar que, nos enfocaremos en el estudio del Crimen Organizado dedicado a actividades de tráfico de drogas; ya que a pesar de que han ido diversificando sus actividades ilícitas, ésta ha sido una actividad determinante para la existencia de muchos de ellos.

II. CONCEPTUALIZANDO A LA DELINCUENCIA ORGANIZADA

Durante los años noventa, el concepto de delincuencia organizada se utilizó como sinónimo de "gansterismo transnacional" o "mafia"; por lo que era utilizado en medios de comunicación y por agentes encargados de diseñar políticas criminales principalmente en Estados Unidos.[4]

Así como el mundo iba evolucionando, las organizaciones criminales también lo hicieron. A partir del último cuarto del siglo XX, las organizaciones criminales aprovecharon la globalización para poder expandir sus actividades a otros países, hasta considerarse una amenaza de carácter transnacional. Por lo que, organismos internacionales comenzaron a involucrarse en la conceptualización de dicho fenómeno.

En el 2000, surgió la Convención de las Naciones Unidas contra la Delincuencia Organizada Internacional, también conocida como la Convención de Palermo. En ella, define el concepto de la siguiente manera:

4 Cordini, Santiago. (2017) "El crimen organizado: un concepto extraño al derecho penal argentino", Universidad de Buenos Aires Argentina, Argentina. Págs.22 PP.4. Véase http://www.scielo.br/pdf/rdgv/v13n1/1808-2432-rdgv-13-01-0334.pdf

> Un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material.[5]

Esta definición se ha replicado en legislaciones de diferentes países, como es el caso de ley mexicana. Algunos de los elementos básicos que predominan en distintas conceptualizaciones realizadas por diversos autores y que nos pueden ayudar a delimitar el concepto son cuatro: participación de un grupo de personas, comisión de una actividad ilegal, la obtención de ganancias económicas y organización. Cabe destacar que este último es la clave para distinguirla de la delincuencia común, la cual, refiere a los actos criminales individuales, sin planeación, en los que no existe una finalidad de permanencia del grupo en caso de cometerse por más de una persona.

III. CONCEPTUALIZANDO EL TÉRMINO DE FRAGMENTACIÓN

Al ser un fenómeno social, las organizaciones experimentan diversos cambios y sus formas de interactuar van siendo distintas. Cabe mencionar que, la literatura relativa a este fenómeno en México es escaza, a pesar de que los autores la perciben como un hecho dentro de su evolución. Al ser considerado un factor que altera factores como el nivel de violencia, la dificultad de su seguimiento e investigación por parte de las autoridades y el mercado, resulta pertinente estudiarlo. Prestarle atención a la temática puede ayudar a tener un mejor entendimiento de las condiciones que propician

---

5 Oficina de las Naciones Unidas Contra la Droga y el Delito (ONUDC), (2004). *"Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus protocolos"*. Nueva York, véase https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

la fragmentación, y así poder estar preparados cuando se presenten esas características, y evitar que los grupos realicen actos violentos.

De acuerdo con Pérez y Atuesta, la fragmentación es una característica inherente a la naturaleza de la delincuencia organizada, y estos a su vez, abordan la literatura de las guerras civiles para definirla como *"una fuerza para explicar la durabilidad y nivel de violencia de un conflicto"*.[6] Para Pealman y Cunningham, la fragmentación se puede concebir como un *"conjunto de procesos que afectan en el tamaño, complejidad e identidad de los grupos"*.[7]

IV. LAS CAUSAS DE LA FRAGMENTACIÓN EN NUESTRO PAÍS Y SU MATERIALIZACIÓN EN VIOLENCIA

La fragmentación se puede dar por varios factores, por lo que, se clasificará en causas internas y externas. Es decir, cuando los factores al interior de la organización causan dicha fragmentación y cuando los componentes externos influyen en su división.

En cuanto a las causas internas, el primer elemento para abordar el fenómeno se realizará desde la perspectiva de la psicología social y el psicoanálisis grupal. El psicoanalista Kurt Lewin afirma que el grupo y su ambiente constituyen un campo social dinámico, cuyos principales elementos son los subgrupos, en donde si un elemento se modifica, se puede modificar la estructura también.[8] Lo anterior, nos ayuda a comprender la importancia de conocer

---

6 Pérez Davila, Samantha., & ATUESTA BECERRA, Laura. (2016). *Fragmentación y cooperación: la evolución del crimen organizado en México* [Ebook] (1st ed.). Aguascalientes: Centro de Investigación y Docencia Económica, p. 12. Véase https://issuu.com/ppdcide/docs/18_fragmentaci__n_y_cooperaci__nfin

7 Pearlman, Wendy, CUNNIGHAM. (2012). *Nonstate actors, Fragmentation and Conflict processes.* Journal of Conflict Resolution. Sage publications. p. 6. Véase http://jcr.sagepub.com/content/early/2011/12/13/0022002711429669

8 Jacobo, María de Lourdes (2012). *Psicología Social y grupos*. Revista Electrónica de Psicología Iztacala. 15, (4), p.1349 Véase
https://www.iztacala.unam.mx/carreras/psicologia/psiclin/vol15num4/Vol-15No4Art10.pdf

las distintas vertientes que surgen dentro de un mismo grupo; ya que resulta complejo mantener una homogeneidad en cuanto a las ideologías, perspectivas, valores, cultura o pretensiones de los miembros pertenecientes a un grupo. Mientras existan vertientes antagónicas dentro de los miembros, mayor posibilidad habrá de que se dé una fragmentación al interior de la organización. La segunda causa interna abordada tiene una alta relación con su estructura organizacional, y responde a la necesidad de los grupos de sobrevivir al no tener estabilidad en sus liderazgos.[9]

Otro factor del cual depende su inclinación a la fragmentación o no, es la identidad de los grupos, mientras más arraigada y poderosa sea, éstos se volverán menos propensos a fragmentarse y, por tanto, a permanecer por más tiempo. Así como también, su forma de organización y estrategias políticas, si éstas son diversas, serán más propensos a fragmentarse.

En cuanto a los factores externos, refieren a cualquier fuerza externa que influya en la estabilidad y permanencia de la organización, estas pueden ser diversas dependiendo el contexto y características; sin embargo, para el caso de la economía ilegal, el autor Garzón Vergara las clasifica en dos fuerzas principales que cambian las dinámicas de las organizaciones criminales, la primera es la fuerza del Estado y la segunda es la del mercado.[10]

De acuerdo con el mismo autor, la fuerza del Estado puede aumentar o disminuir el riesgo para las organizaciones de realizar

---

9 Galvano Quiroga, Melisa. (2014) *Narcotráfico en México ¿Quisieron combatirlo y lo terminaron sembrando?,* (Ebook). Editorial Dunken, Argentina. Véase en https://books.google.com.mx/books?id=B3aJBAAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

10 Garzón Vergara, Juan Carlos (2014). From Drug Cartels to Predatory Micro-Networks: the "new" face of organized crime in Latin America, en Bagley, Bruce M, Rosen, Jonathan y Kassab, Hannah, Reconceptualizing Security in the Americas in the Twenty-First Century, Lanham, Lexington Books, p.8, véase https://www.academia.edu/17053036/From_Drug_Cartels_to_Predatory_Micro_Networks_the_new_face_of_organized_crime_in_Latin_America

una actividad ilegal, lo cual causará cambios en su comportamiento.[11] Pérez y Atuesta coinciden en esta misma teoría argumentando que una de las causas de la fragmentación han sido las estrategias de seguridad de las autoridades, y la fragmentación ha sido una forma de respuesta de los grupos. Tal es el caso del ataque y desmantelamiento del grupo terrorista Al-Qaeda por parte de Estados Unidos, el cual provocó la fragmentación del grupo, creando a partir de ésta, la aparición de aproximadamente 32 grupos terroristas en Siria.

En el caso de México, la estrategia de seguridad implementada entre 2006 y 2012, fue un factor fundamental. Se basó en la estrategia de captura de capos o líderes de las organizaciones criminales, también conocida como *"The Kingpin Strategy"* por su nombre en inglés. Esta estrategia tiene por objetivo el desmantelamiento de los grupos dedicados al tráfico de drogas a través de la ejecución o captura de sus líderes, bajo la premisa de que al remover a los líderes la organización, esta se vería dañada y debilitaría el ciclo del tráfico de drogas.

De lo anterior, podemos concluir que, las autoridades mexicanas realizaron un trabajo aparentemente exitoso al neutralizar a la mayoría de los líderes buscados, específicamente al 64%. De este porcentaje, detuvieron al 43% y ejecutaron al 16%. La segunda cifra podría resultar negativa en términos de sus implicaciones, ya que, existe la posibilidad de que una ejecución torne más violenta la transición del cártel que ha quedado sin mando, éste resulta ser más violento tanto en la competencia interna por tomar el mando de la organización, como al exterior; ya que intenta vengar el asesinato de su líder realizando actos violentos en contra de las mismas autoridades y a veces en contra de la sociedad. Por el contrario, cuando se hace por medio de una detención, la transición posiblemente resulta ser más lenta, paulatina y menos violenta.

Si bien es cierto que las medidas anteriormente mencionadas

11 Ibidem

afectaron la continuidad y el desarrollo de las actividades de las organizaciones criminales, e incluso aumentaron sus costos operativos, es posible observar que no reducen la violencia ni el tráfico de drogas en el mediano plazo.

El impacto positivo de las capturas fue mínimo, por el contrario, generó desbalances en la correlación de las fuerzas entre los cárteles de Sinaloa, Juárez y del Golfo. Las organizaciones mutaron, diversificaron sus actividades y se fragmentaron. No se logró erradicar el negocio ni la existencia de las organizaciones, únicamente generó cambios en su comportamiento, ya que se vieron obligados a buscar nuevas estrategias.

El segundo factor de cambio reitera la importancia de la fuerza de los mercados, es decir, los cambios que se han dado en la oferta y la demanda de dichas sustancias, así como los cambios en los tipos de estupefacientes que lanzan las organizaciones al mercado. Derivado de que, el beneficio económico es el principal incentivo para quebrantar la ley para las organizaciones criminales, se incrementa la competencia y cooperación entre los grupos, personas e incluso instituciones.[12]

Al hacer un análisis de las cifras de la demanda de marihuana en Estados Unidos, se puede observar que, a pesar su aumento, hubo una caída en el trasiego de esta droga por parte de los cárteles mexicanos hacia el país norteamericano. A partir del año 2013, cayó de manera abrupta el tráfico a dicho país. Cabe mencionar que, el año anterior, el 6 de noviembre de 2012, se aprobó la legalización para el consumo recreativo de la marihuana en algunos estados de Estados Unidos como Colorado y Washington.[13] Por lo anterior, se podría inferir que, el contexto influyó en la fragmentación de las organizaciones, debido a que el mercado se tornó más pequeño para México, y por tanto, más cárteles querían competir ese mercado.

---

12 Ibidem

13 Editorial Board (2014) *Repeal Prohibition, Again*. New York Times. Disponible en: https://nyti.ms/2jRQGj4

Sin embargo, los cárteles mexicanos comenzaron a distribuir y vender en México, la marihuana que no consumían los norteamericanos, por lo que se observa un incremento en el consumo de dicha droga en México. De acuerdo con la Secretaría de Salud, en el 2002, 3.5 millones de mexicanos consumieron marihuana, mientras que, para el 2016 ya eran 8.6 millones. Sin embargo, esta alternativa no fue la única que tomaron los cárteles, ya que, comenzaron a incursionar en el mercado de las drogas sintéticas como el fentanilo.

Al analizar las consecuencias que la fragmentación puede desencadenar, las teorías son diversas. Autores como Driscoll, destacan que el fenómeno de la fragmentación es favorable para su ataque y desarticulación; ya que permite que el gobierno divida a los líderes y los coopte con el fin de establecer la paz, provocando menos estabilidad en su organización.[14] Por su parte, Pearlman y Cunningham, argumentan que uno de los efectos o consecuencias de la fragmentación, es la violencia, ya sea hacia el Estado o entre los grupos, debido a que el surgimiento de nuevos actores es un incentivo para utilizar la violencia en contra de sus enemigos.

Podemos considerar a la fragmentación como una fuerza que también altera el grado de intento de cooptación de las autoridades por parte de la delincuencia organizada. Según Staniland, la competencia letal entre los grupos puede culminar en la deserción de algunos, por lo que sólo algunos sobreviven, y éstos que sí sobreviven se encuentran debilitados, acudiendo a la protección del Estado para garantizar su continuidad.[15]

Además, de acuerdo con el modelo propuesto por Fiorentini, las organizaciones criminales invierten en la realización de actividades

14 Pearlman, Wendy, CUNNIGHAM. (2012). Nonstate actors, Fragmentation and Conflict processes. Journal of Conflict Resolution. Sage publications. (Artículo) Págs. 15, Véase en: http://jcr.sagepub.com/content/early/2011/12/13/0022002711429669.citation)

15 Staniland, Paul. (2012). Between a Rock and a Hard Place: Insurgent Fratricide and Ethnic Defection in Kashmir and Sri Lanka. Journal of Conflict Resolutions. Sage Publications, Véase en: https://journals.sagepub.com/doi/abs/10.1177/0022002711429681

violentas con la finalidad de reducir los costos de transacción en el mercado donde venden el producto ilícito. Esto se puede observar en distintos actos violentos como asesinatos cometidos en contra de servidores públicos o presidentes municipales, con la finalidad de causar miedo y mostrar autoridad, logrando así, disminuir costos derivados de los sobornos y corrupción para realizar con éxito sus actividades criminales.

Por su parte, las Organizaciones Criminales emplean la violencia como un mecanismo mediante el cual pueden asegurarse del cumplimiento de los acuerdos que realizan entre ellos, es decir, hacen justicia por su propia mano, según la autora Letizia Paoli.

Existen tres tipos de violencia relacionada con la delincuencia organizada. La primera, refiere a la violencia externa, es decir, por parte de las organizaciones criminales hacia el gobierno, la cual parece ser un intento de establecer impunidad; mientras que, la segunda es la violencia "inter-cárteles", la cual pretende dominar ciertas "plazas" o territorios de tráfico o producción de droga, y finalmente, está la categoría "intra-cárteles", la cual sucede al interior de las organizaciones, usándose como una respuesta ante la sospecha de que un miembro traicionó o podría traicionar a la organización, dándole información a la competencia para superar, matar o arrestar a alguno de sus líderes.

De acuerdo con lo mencionado anteriormente por distintos autores, se podría inferir que la violencia es una característica sin la cual no puede existir un grupo de la delincuencia organizada; pues la han utilizado a través de la historia para posicionarse como el grupo más poderoso y violento, por lo que termina siendo un instrumento de control; sin embargo, es importante no perder de vista que las organizaciones tienen fines económicos y la violencia representa un gasto considerable para ellos.

Al materializar estos cambios, podemos observar que, la acción del Estado ha provocado un proceso de fragmentación de las estructuras criminales, el cual ha sido acompañado de las siguientes tendencias:

cambio en rutas de tráfico de droga, desarrollo de mercado interno de consumo de drogas, cambio en patrones de consumo y diversificación de actividades, esto orientado al incremento de sus ingresos.

Además, en términos de violencia, han incrementado los enfrentamientos de los grupos de la Delincuencia Organizada en México, el índice de letalidad y la diversificación de actividades por parte de los grupos que surgen de la fragmentación. Al analizar los estados en los que hay una mayor cantidad de cárteles, tambien se observa un mayor nivel de violencia y número homicidios, como lo son Chihuahua, Durango y Sinaloa, donde se encuentra el Triángulo Dorado, así como Guerrero, Michoacán, México, Jalisco, Guanajuato y Morelos, lugares importantes en la ruta, producción, y tráfico de drogas.

Por su parte, los enfrentamientos entre civiles armados y militares o policías también se han convertido en eventos cada vez más frecuentes. De acuerdo con datos aportados por la Secretaria de la Defensa Nacional (SEDENA), en 2008 hubo alrededor de 5.1 civiles muertos por cada soldado que moría en los enfrentamientos, mientras que en 2011 la proporción fue de 32.4 civiles por cada militar.[16] Estas cifras aumentaron durante la administración de Calderón y existe la posibilidad de que hayan sido resultado de la fragmentación de los grupos de la Delincuencia Organizada, ya que un mayor número de organizaciones supone un elevado nivel de violencia y, por tanto, de enfrentamientos. Sin embargo, la respuesta violenta por parte de las autoridades genera a su vez más violencia y contribuye a la formación de una espiral de esta.

El tercer elemento por analizar es la diversificación de actividades ilícitas, la cual también es una forma de violencia que ha tenido un gran impacto en la sociedad, debido a que son las víctimas directas de las actividades delictivas a las que se diversifican. Además,

16 Forne, Silva, Perez, Carolina, et al (2017) índice de letalidad 2008-2014: menos enfrentamientos, misma letalidad, más opacidad. Perfiles Latinoamericanos 25, p.4 Véase en: http://www.scielo.org.mx/pdf/perlat/v25n50/0188-7653-perlat-25-50-00331.pdf

tiene un alto impacto en la economía, ya que brinda inestabilidad al sector de inversión nacional y extranjera, merma los ingresos de los ciudadanos y las empresas afectadas y en algunos casos impide su perpetuidad.

De acuerdo con Guerrero, la fragmentación de las organizaciones grandes causa una expansión de la violencia a nuevos municipios, a la par de esta también crece la delincuencia, la extorsión, secuestro y tráfico de personas. A diferencia de los cárteles, las organizaciones menores no poseen los recursos suficientes para traficar drogas, como contactos e infraestructura logística, por lo que emprenden actividades ilícitas que son menos lucrativas; sin embargo, estas actividades se convierten en unas más violentas, depredadoras y extractivas.[17]

El segundo comportamiento, podría referirse a los grupos dedicados al tráfico de drogas que no lograron adaptarse a los cambios, es decir, a la reducción del consumo de marihuana mexicana o consumo de cocaína, o bien, que solo realizan una de las etapas en el tráfico de drogas transnacional; pero que no consideran suficientes sus ingresos, y prefieren dedicarse a otro tipo de actividades ilícitas como el secuestro, el robo, extorsión, asalto, entre otros.

El ámbito local de los mercados ilegales ofrece algunos beneficios para las organizaciones, como el de la disponibilidad de flujo de efectivo y de una base social construida por la contratación de una fuerza laboral local. Además, los mercados locales sirven para interactuar con el sector informal y eventualmente abrir una oportunidad para entrar a la economía formal.[18]

---

17 Fernandez de Lara, Alfredo. (2017) Análisis de la Estrategia de Blancos Prioritarios para la contención y debilitamiento de los Cárteles y la reducción de la violencia en México (2000-2016). Véase en: http://www.congresoalacip2017.org/arquivo/downloadpublic2?q=YToyOntzOjY6InBhcmFtcyI7czozNToiYToxOntzOjEwOiJJRF9BUlFVSVZPIjtzOjQ6IjI3MjEiO30iO3M6MToiaCI7czozMjoiMzQwMmE0OWRmYzgxMmIzNjFiZWVhZGU0ZDBiMjU2NTMiO30%3D

18 Garzón Vergara (2014) Óp. Cit., p. 4-5

V. LA AGENDA PRESIDENCIAL DE SEGURIDAD EN MÉXICO PARA EL COMBATE A LA INSEGURIDAD

Ante la problemática definida en el texto, resulta imperioso abordar el tema de la agenda presidencial de Seguridad en México y los esfuerzos realizados en la materia.

Los dos ejes de la agenda discursiva del Presidente López Obrador para su gestión 2018-2024, fueron el combate a la inseguridad y la corrupción. En términos de las reformas que ha emprendido visualizamos la disolución de la Policía Federal y la creación de la Guardia Nacional. En cuanto a la inteligencia civil, se creó el Centro Nacional de Inteligencia hoy adscrito a la Secretaría de Seguridad y Protección Ciudadana y desapareció el Centro de Investigación y Seguridad Nacional. En la actualidad los asuntos de seguridad nacional se operan desde una secretaría que atiende asuntos de seguridad pública. Se rompe con una tradición que al menos tenía un precedente desde 1989 en dar seguimiento a acciones de inteligencia civil desde la Secretaría de Gobernación. Los efectos los evaluaremos conforme pase el tiempo, sin embargo, no abona a la tarea pendiente de crear y consolidar una comunidad de inteligencia en el país y de dibujar una delimitación entre lo que el gobierno entiende por seguridad nacional y pública.

La creación de la Guardia Nacional y su ley respectiva surgen el 2 de mayo de 2019 y podemos describirla como un órgano civil con funciones policiales y estructura militar. Su breve tiempo de operación, ha puesto de manifiesto los retos que enfrenta en materia de reclutamiento, profesionalización, directrices en el uso de la fuerza y en el respeto de los derechos humanos en un esquema que transita en el nombre únicamente a un enfoque de seguridad ciudadana. La reforma policial quedó condenada a su estancamiento, en vista de que ha sido más funcional la participación de militares en el combate a las actividades del crimen organizado. En entornos democráticos, se espera tener una policía cercana a los ciudadanos y la realidad

pone de manifiesto un alejamiento y un abandono por restaurar las capacidades institucionales de esta importante institución. En las entidades federativas se pueden celebrar acuerdos con autoridades estatales con remuneración para solicitar la protección y presencia de la Guardia Nacional. Esto crea un incentivo perverso para que los gobernadores dejen de invertir en sus propias policías estatales condena fortalecimiento de capacidades institucionales de las mismas.

Además, en términos presupuestales, México presenta el menor nivel de gasto en seguridad interna y sistema judicial de los 33 países de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), con 0.7% del PIB.

Estamos visualizando una difícil consolidación del énfasis en la prevención, la protección de derechos humanos y las prácticas de transparencia inherentes a una versión democrática de la reforma policial y de la seguridad. En mayo de 2020, se publicó el Decreto del Presidente López Obrador con relación a la participación de las Fuerzas Armadas en tareas de seguridad pública hasta 2024. La Comisión Interamericana de Derechos Humanos estableció en su Informe Anual 2019 una especial preocupación por el elevado nivel de desapariciones y homicidios sin debida investigación.

Por su parte, la relación bilateral entre México y Estados Unidos ha jugado un papel fundamental. Siempre ha sido un termómetro de asimetrías, desavenencias y acuerdos entre ambos países, especialmente en temas de economía y seguridad. A fines del mes de noviembre de 2019, el Presidente Trump amenazó con denominar a los cárteles de la droga mexicanos como grupos terroristas. Sin embargo, el tema se quedó en el tintero de este mandatario, como un titular a nivel mediático y posteriormente dijo que se analizaría en otro momento esta situación. El gobierno actual ha cumplido su promesa de contener migrantes a través del trabajo en la frontera sur de la Guardia Nacional.

VI. CONTEXTO ACTUAL DE LA DELINCUENCIA ORGANIZADA EN EL MARCO DE LA EMERGENCIA SANITARIA POR COVID-19

Actualmente, la violencia en México continúa incrementándose y no se ha detenido con la pandemia del COVID-19. De acuerdo con el Índice de Paz 2020, el Estado mexicano enfrenta una grave problemática:

- El homicidio es la principal causa de muerte en jóvenes mexicanos entre las personas de 15 a 44 años, y la cuarta más frecuente entre niños de cinco a 14 años.
- En 2019, el nivel de paz en México tuvo un retroceso de 4.3%, descendiendo por cuarto año consecutivo. Este deterioro se debió a que las actividades delictivas se incrementaron de manera importante, al grado que la tasa de crímenes de la delincuencia organizada creció 24.3%.
- Desde 2015, la tasa de homicidios se ha elevado 86%
- El impacto económico de la violencia en México se calculó en 238 mil millones de dólares en 2019, cifra equivalente a 21.3% del PIB nacional.[19]

Especialmente, las organizaciones dedicadas al tráfico ilícito de drogas se vieron afectadas en distintas etapas de su cadena de suministro y venta durante la pandemia. La producción de drogas sintéticas se vio afectada debido a que la llegada de precursores químicos por medios marítimos disminuyó, ya que el tráfico de productos lícitos también lo hizo. Lo mismo sucedió en la frontera con el país norteamericano para el trasiego de drogas, las restricciones impuestas por los países tornaron más complicado y riesgoso el proceso. Finalmente, la venta también se ha visto afectada, ya que, los centros nocturnos donde se distribuye gran parte de ésta se vieron obligados a cerrar. Sin embargo, es probable

19 Índice de Paz México 2020: Identificar y medir los factores que impulsan la paz, Sidney, abril de 2020. Disponible en: indicedepazmexico.org.

que cuando la movilidad comience a normalizarse, las actividades delictivas también lo hagan e incrementen.

La pandemia se enmarca en una crisis dentro de otra crisis, que es la de la Globalización. Es decir, ya venía un proceso de desaceleración económica mundial, una interrupción en las cadenas de suministro donde las interdependencias se vieron interrumpidas. De acuerdo con Sanhauja, la pandemia de COVID-19 puede verse como una "coyuntura crítica" que exacerba y agudiza las dinámicas presentes en otra crisis, anterior, más amplia, y de más lento desarrollo: la crisis de las estructuras históricas –materiales, institucionales, ideacionales– sobre las que se ha sustentado la globalización y el orden internacional liberal.[20]

VII. CONCLUSIONES

En México, observamos que, cuando el Estado aumentó sus esfuerzos en el combate al crimen, este último también aumentó sus esfuerzos, en armento, poder de fuerza y violencia. Se denomina traslado del costo, por lo que, en este caso el costo se trasladó a las víctimas. No es posible atribuir a una sola causa el fenómeno de la fragmentación, si bien se han analizado algunas de ellas, es importante tomar en consideración que estas sólo constituyen piezas importantes para entender el fenómeno en su totalidad, y no pretenden restarles importancia a factores como la debilidad institucional o la corrupción.

Al recordar que la fuerza del mercado de drogas genera ganancias para el crimen y la fuerza del estado costos, se observa que los grupos delincuenciales tienen una alta capacidad de adaptación, han modificado su forma de operación, estructura, generación de ganancias e incluso el ejercicio de la violencia; pero el cambio nun-

20 Sanahuja, José Antonio. "Covid-19: riesgo, pandemia y crisis de gobernanza global" en Mesa, Manuela (Coord). "Riesgos globales y multilateralismo: el impacto de la COVID-19.", Ceipaz, Madrid, 2020, p.29, véase https://ceipaz.org/anuario/anuario-2020/

ca implicó su desaparición.

La fragmentación causó conflictos al interior de los grupos, lo cual provocó de nuevo fragmentación y ésta a su vez, causó conflictos entre los grupos, lo cual torna este proceso en una espiral que genera cada vez más violencia y no termina. La operación en el ámbito local de cárteles con menores recursos ha provocado más violencia. Una mayor competencia ha traído diversificación, especialmente en el ámbito local y el incremento de delitos patrimoniales y de robo de recursos de la nación. Posiblemente, se han incrementado estos delitos para financiar los brazos armados de los cárteles, ya que la dinámica y fuerzas los han obligado a incrementar también el uso de violencia. Algunos otros que también son resultado de la fragmentación, probablemente sólo realizan delitos de bajo impacto. A pesar de los esfuerzos, según informes de Estados Unidos, los cárteles monopólicos continúan y algunos subcontratan a algunos más pequeños que han surgido de la fragmentación.

Es imprescindible partir del supuesto de que, los cárteles y organizaciones criminales son distintas, tienen diferentes capacidades, recursos, ideología, procesos, especialización y estructuras, por lo que se propone realizar estrategias locales y regionales. Resultaría impreciso pensar que todos los cárteles son iguales y que por ello una estrategia nacional dirigida a todos, puede desarticularlos. Si no se conocen sus particularidades, no se conocerán sus debilidades y, por tanto, resultará complicado hacerles frente. Si se parte del supuesto de que los cárteles pretenden sobrevivir, el primer paso sería enfocarse en reducir su capacidad y sus procesos, y una vez que se logre, eliminarlos.

La pandemia generó un impacto en cadenas de suministro, así como una interrupción en la producción de laboratorios clandestinos por el cierre parcial de frontera con los Estados Unidos, y los envíos se han hecho vía marítima.[21] Asimismo, diversos grupos criminales

21 Olson Eric, Violent non-state actors and Covid-19. Challenge or Opportunity, Part 1. Wilson Center, 26 de mayo de 2020, véase https://www.youtube.com/watch?v=BJZKinyCUKg&list=LL&index=6&t=1450s

repartieron despensas en medio de la pandemia a grupos vulnerables como un proceso de legitimación de sus actividades y presencia en zonas vulnerables. Esta es una línea de investigación futura para el estudio de generación de combate de políticas al crimen organizado que incluyan el apoyo de una amplia base social, donde el Estado ha dejado de tener presencia.

Las estrategias se podrían realizar con base en el contexto de cada uno de los cárteles para lo cual se requiere analizar la base social de donde operan y surgen los mismos. Para ello, es indispensable adelantase al fenómeno, conocer el movimiento que realizarán antes de que lo hagan, y ello sólo se logrará a través del fortalecimiento de inteligencia, acompañado de esfuerzos de una mejora de instituciones en materia de seguridad y del fortalecimiento de las capacidades institucionales. Se debe tener en cuenta, la importancia de la prevención, investigación, judicialización y castigo del delito. Si falla alguna de las etapas, resultará complicado combatir este fenómeno.

VIII. FUENTES DE CONSULTA

Bibliografía

Cordini, Santiago. (2017) "El crimen organizado: un concepto extraño al derecho penal argentino", Universidad de Buenos Aires Argentina, Argentina. Págs.22 PP.4. Disponible en: http://www.scielo.br/pdf/rdgv/v13n1/1808-2432-rdgv-13-01-0334.pdf

Fernandez de Lara, Alfredo. (2017) Análisis de la Estrategia de Blancos Prioritarios para la contención y debilitamiento de los Cárteles y la reducción de la violencia en México (2000-2016). Págs. 32 Disponible en: http://www.congresoalacip2017.org/arquivo/downloadpublic2?q=YToyOntzOjY6InBhcmFtcyI7czozNToiYToxOntzOjEwOiJJRF9BUlFVSVZPIjtzOjQ6IjI3MjEiO30iO3M6MToiaCI7czozMjoiMzQwMmE0OWRmYzgxMmIzNjFiZWVhZGU0ZDBiMjU2NTMiO30%3D

Forne, Silva, Perez, Carolina, et al (2017) índice de letalidad 2008-2014: menos enfrentamientos, misma letalidad, más opacidad. Perfiles Latinoamericanos 25 pp.4 Pags. 29. Disponible en: http://www.scielo.org.mx/pdf/perlat/v25n50/0188-7653-perlat-25-50-00331.pdf

Galvano Quiroga, Melisa. (2014) *Narcotráfico en México ¿Quisieron combatirlo y lo terminaron sembrando?,* (Ebook). Editorial Dunken, Argentina. Págs. 97 Véase en: https://books.google.com.mx/books?id=B3aJBAAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Garzón Vergara, Juan Carlos (2014). From Drug Cartels to Predatory Micro-Networks: the "new" face of organized crime in Latin America, en Bagley, Bruce M, ROSEN, Jonathan y KASSAB, Hannah, Reconceptualizing Security in the Americas in the Twenty-First Century, Lanham, Lexington Books. Págs. 8. Véase en: https://www.academia.edu/17053036/From_Drug_Cartels_to_Predatory_Micro_Networks_the_new_face_of_organized_crime_in_Latin_America

Jacobo, María de Lourdes (2012). *Psicología Social y grupos*. Revista Electrónica de Psicología Iztacala. 15, (4), Págs. 11, Véase en: https://www.iztacala.unam.mx/carreras/psicologia/psiclin/vol15num4/Vol15No4Art10.pdf

Le Gloannec, Anne-Marie, Irondelle, Bastien, and Cadier, David, eds. (2013), "New and Evolving Trends in International Security", Transworld Working Papers, No.13 (April), p.10, véase http://www.transworld-fp7.eu/?p=1175

Pérez Dávila, Samantha., & Atuesta Becerra, Laura (2016) *Fragmentación y cooperación: la evolución del crimen organizado en México* [Ebook] (1st ed.). Aguascalientes: Centro de Investigación y Docencia Económica, p. 12. Véase en: https://issuu.com/ppdcide/docs/18_fragmentaci__n_y_cooperaci__nfin

Olson, Eric. Violent non state actors and Covid-19. Challenge or Opportunity, Part 1. Wilson Center, 26 de mayo de 2020, véase https://www.youtube.com/watch?v=BJZKinyCUKg&list=LL&index=6&t=1450s

Pearlman, Wendy, Cunnigham. (2012). Nonstate actors, Fragmentation and Conflict processes. Journal of Conflict Resolution. Sage publications, Págs. 15, véase en: http://jcr.sagepub.com/content/early/2011/12/13/0022002711429669.citation

Ruiz, Arcelia, García, Tonatiuh, Blázquez, Ferrán, Sahagún, Ángel. (2016) *El Sicariato: una perspectiva psicosocial del asesinato por encargo*. Universidad de Guanajuato, México. Revista Electrónica de Psicología Iztacala, Vol.9 No.3, Págs.20 Véase en: https://www.iztacala.unam.mx/carreras/psicologia/psiclin/vol19num3/Vol19No3Art8.pdf

Sanahuja, José Antonio. "Covid-19: riesgo, pandemia y crisis de gobernanza global" en Mesa, Manuela (Coord). "Riesgos globales y multilateralismo: el impacto de la COVID-19.", Ceipaz, Madrid, 2020, p.29, véase https://ceipaz.org/anuario/anuario-2020/

Staniland, Paul. (2012). Between a Rock and a Hard Place: Insurgent Fratricide and Ethnic Defection in Kashmir and Sri Lanka. Journal of Conflict Resolutions. Sage Publications, Disponible en: https://journals.sagepub.com/doi/abs/10.1177/0022002711429681

Informes y Documentos

CEPAL. Informe especial Covid-19, 12 de mayo de 2020, véase https://repositorio.cepal.org/bitstream/handle/11362/45527/5/S2000325_es.pdf

Editorial Board (2014*) Repeal Prohibition, Again*. New York Times. Disponible en: https://nyti.ms/2jRQGj4

Global Trends 2025: A transformed World, Office of the Director of National Intelligence, 2008, p. 75 véase https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2025_Global_Trends_Final_Report.pdf

Índice de Paz México 2020: Identificar y medir los factores que impulsan la paz, Sidney, abril de 2020. Disponible en: indicedepazmexico.org.

Oficina de las Naciones Unidas Contra la Droga y el Delito (ONUDC),

(2004). *"Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus protocolos"*. Nueva York. PP.5 Disponible en: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

LOS RETOS DEL DERECHO ANTE LAS NUEVAS TECNOLOGÍAS COMO GENERADORAS DE CONDUCTAS DELICTIVAS

Luis Ángel Morales Cortez*
Lidia Chávez Fonseca**

SUMARIO: I. Introducción; II. Derecho de las Nuevas Tecnologías; III. La Política Criminal y su tratamiento en los Delitos Informáticos; IV. La relación de las TIC con el surgimiento de nuevas conductas delictivas; V. Retos; VI. Conclusiones; y VII. Fuentes de Consulta.

I. INTRODUCCIÓN

El avance de la tecnología ha ocasionado que la sociedad hoy en día utilice con mayor frecuencia las tecnologías de la información y comunicación (TIC), en diversas actividades como la educación, la economía, la cultura, la política, entre otras; esto con la finalidad de agilizar los procesos en tiempo real, rompiendo las fronteras físicas, culturales y del idioma para beneficio de las personas, instituciones y gobiernos.

Si bien las tecnologías de la información y comunicación son un beneficio para la sociedad, su utilización ha ocasionado que el derecho tenga que actualizarse en el uso de estas, lo que ha generado nuevos conceptos como Derecho de las nuevas tecnologías, la cual tiene como objeto todo lo que involucra el uso de estas, como el uso

* Especialista en Derecho Penal y Maestro en Derecho por la Universidad Nacional Autónoma de México (Facultad de Estudios Superiores Acatlán) y catedrático de la Licenciatura en Derecho en la Universidad Nacional Autónoma de México (Facultad de Estudios Superiores Acatlán).
** Estudiante de la Especialidad en Derecho Energético y Maestra en Derecho por la Universidad Nacional Autónoma de México (Facultad de Estudios Superiores Acatlán) y catedrática de la Licenciatura en Derecho en la Universidad Nacional Autónoma de México (Facultad de Estudios Superiores Acatlán).

del internet, los contratos vía electrónica, contratación electrónica, protección de información y base de datos, comercio electrónico y los *ciberdelitos* o delitos informáticos, en este sentido estos últimos han tenido una gran trascendencia, toda vez que son más comunes derivado a la falta de regulación y de seguridad en los sistemas informáticos, muchas de las conductas que han surgido son el *Ciberbullying*, el secuestro de información, el robo de identidad, el *sexting*, el *phising*, piratería de programas informáticos, acceso ilícito de sistemas informáticos, fraude informático, interferencia de datos, etcétera, por mencionar solo algunos ya que hay una gran cantidad de conductas relacionadas a la utilización de tecnologías.

La mayoría y los principales *ciberdelitos* o delitos informáticos son en contra de los particulares, pero los más grandes en afectaciones económicas son en contra de las grandes corporaciones e instituciones gubernamentales, por lo que la cooperación internacional es de suma importancia para establecer instrumentos internacionales en materia de *ciberseguridad*, que deben de convergen con las legislaciones federales y locales de cada uno de los países, en que cada uno de estos el dinamismo de la norma sea igual de exponencial a los cambios tecnológicos y a las conductas que surgen de estas, basado en una Política Criminal/*Cibercriminal*.

II. DERECHO DE LAS NUEVAS TECNOLOGÍAS

Sin duda alguna el avance de la tecnología ha ayudado al desarrollo humano y a satisfacer ciertas necesidades que sin ella pudieran ser más complicadas, además ha impactado en prácticamente todas las actividades del ser humano, desde la creación de los primeros utensilios en la prehistoria, hasta lo más avanzado hoy en día, tan solo cabe mencionar que ha facilitado la comunicación, la industria y las ciencias.

De acuerdo a lo anterior, la tecnología ha ayudado al desarrollo de las prácticas profesionales, como en los procedimientos médicos, la educación y demás, pero particularmente en el derecho, en el

cual se puede observar desde la práctica, regulación de las mismas, así como el de nuevas conductas que surgen por su utilización, lo cual se plantea más adelante.

En un sentido genérico se ha mencionado a la tecnología, sin embargo en el afán de tratar de englobar todo lo que tiene que ver con el desarrollo de los nuevos avances en dicha área, surge lo que son las tecnologías de la información y comunicación lo cual "se refiere a las múltiples herramientas tecnológicas dedicadas a almacenar, procesar y transmitir información, haciendo que ésta se manifieste en sus tres formas conocidas: texto, imágenes y audio"[1], de acuerdo a lo anterior prácticamente se hace referencia a todas las herramientas que se conocen hoy en día, como los dispositivos electrónicos e inteligentes, conexiones, *software*, etcétera, esto con la finalidad de que la información pueda ser compartida y facilitar las actividades del ser humano, por lo que además ha impulsado otros sectores como el comercio y el gobierno, esto último:

> Empoderan a los ciudadanos, ya que pueden fortalecer la participación ciudadana y la configuración de la democracia en la medida en que se acerca los gobernados con sus gobernantes y facilita la recopilación, difusión e intercambio de información pública relevante para sus ciudadanos.[2]

De acuerdo a lo anterior, se puede observar la importancia de las tecnologías, ya que a través de ellas con el llamado gobierno electrónico o *e-gobierno*, han facilitado la interacción entre el gobierno y los gobernantes, sobre todo en los tramites, ya que ayuda a reducir los recursos materiales y humanos, tiempos de procedimientos y agilidad en ellos, por ejemplo hoy se puede observar la facilidad para realizar pagos de impuestos, tramites de documentos

---

1 Zambrano Martínez, Fernando, *Las TICS en nuestro ámbito social*, recuperado en: http://www.revista.unam.mx/vol.10/num11/art79/int79.htm, consultado el 20 de mayo de 2020.

2 Villanueva, Ernesto y Díaz, Vanessa, *Derecho de las Nuevas Tecnologías,* México. Oxford, 2015, p. 6

como el CURP, constancias fiscales, actas de nacimiento, cedulas profesionales, entre muchos otros. Pero aún más lejos de este de procedimientos las tecnologías han ocasionado incluso un cambio en los procesos electorales, los cuales han utilizado a las tecnologías como un medio para las campañas, pues como se sabe y de manera específica los usos de las Redes Sociales han sido determinantes en elecciones presidenciales, tal es el caso de las elecciones del 2016 en los Estados Unidos o han ayudado al uso mediático de la información lo que pasa en México y en muchos países del mundo.

El derecho de las nuevas tecnologías hay que entenderlo desde tres sociedades, la primera de ellas se refiere a la sociedad de la información, la cual señala que:

> Las tecnologías que facilitan la creación, distribución y manipulación de la información, juegan un papel esencial para las actividades sociales, culturales y económicas. La noción de la sociedad de la información ha sido inspirada por los programas de desarrollo de los países industrializados. Organismos desde el lugar y en la forma en que se prefiera, ya sea por las páginas de internet o sitios web.[3]

Este tipo de sociedad ve como principal elemento a la información, ya que a través de esta es capaz de proveer productos, hasta conceptualizar ideas políticas, culturales, económicas, etcétera, pues el manejo de la información es una herramienta fundamental en el desarrollo del ser humano de manera individual y colectiva.

Por lo que en este caso las tecnologías juegan un papel fundamental ya que:

> Faculta al ser humano para hacer provecho de datos, información y conocimiento en formas, modos o maneras sin precedentes propiciando un intercambio científico cultural y técnico a escala mundial, pasando sobre las barreras geográficas, las visiones políticas y las del tiempo, propiciado por la globalización, primero económica

3 García Barrera, Myrna Elia, *Manual de Derecho de las Nuevas Tecnologías*, México, Tirant lo Blanch, 2018, p. 27.

y luego cultural.[4]

En este sentido se han roto todas las barreras de comunicación que se conocían, por lo que las tecnologías han facilitado la interacción de las personas sin importar la distancia o incluso el lenguaje creando herramientas para poder comunicarse.

Otra sociedad de igual trascendencia es la del conocimiento, la cual sabe de la importancia del uso de las Tecnología de la Información y la Comunicación, dicha sociedad, además:

> se necesita para competir y tener éxito frente a los cambios económicos y políticos del mundo moderno, se caracteriza porque el conocimiento es el principal componente de cualquier actividad, ya sea económica, social, cultural. La información y el conocimiento son el principal recurso de toda actividad y también se constituyen en un producto, Esta sociedad considera a la Tecnologías de la Información y Comunicación (TIC) como un factor de cambio social, entre otros. Es una sociedad consiente del no-saber y de los riesgos de lo que esto implica.[5]

Después de la revolución industrial y el paso a la revolución tecnológica, esta última se ha convertido en el principal factor en la economía mundial, ya que por medio de las tecnologías ya sea como producto, como un medio de manufactura o un medio por el cual se ofrecen los productos, es la mayor industria en el mundo, que a través de ella han surgido importantes cambios sociales, culturales y políticos.

Es importante señalar que este tipo de sociedad consiente del conocimiento y de su importancia como factor en este tipo de cambios, que además es: "Caracterizada por la utilización extensiva de las tecnologías de la información (TIC) que hacen posible un almacenamiento y una gestión de datos y de conocimiento"[6]

---

4 *Ibídem*, p. 28.
5 *Ibídem*, p. 27.
6 *Ibídem*, p. 28.

Un conocimiento que se genera por medio de habilidades, experiencias adquiridas y que son de suma importancia para el desarrollo de las tecnologías y que a su vez permiten su resguardo, pues basta con ver la cantidad de datos que se encuentra en los recursos o redes y en sus servidores para darse cuenta de su importancia.

Por último, también existe la llamada sociedad de redes, la cual:

> Está construida por redes de información que procesan, almacenan y transmiten información sin estricciones de distancia, tiempo ni volumen. Esta nueva forma de entender el funcionamiento de la sociedad se basa en el fenómeno de la globalización, el cual se ha ido desarrollando gracias a la internet. Estructura social hecha de redes de información características del paradigma informacionalista.[7]

Sin esta sociedad, no sería posible la transmisión de la gran cantidad de información que circula a través del internet, pues de manera concreta se puede obtener o compartirla, prácticamente de manera instantánea en cualquier lugar del planeta donde se tenga acceso a una red.

Se puede decir que es la sociedad más importante, ya que sin esta no podría compartirse la información ni su almacenamiento, se dice que:

> Es la estructura social de nuestro tiempo. Es, simplemente, la sociedad en la que hemos ido entrando desde hace algún tiempo, en un proceso de transición a partir de la sociedad industrial en la que vivimos durante más de un siglo, aunado a la sociedad de la información que ha permitido la interconectividad de personas, en donde somos constructores de la propia información y conocimiento. [8]

Por lo que en su conjunto estas tres sociedades, son esenciales para el desarrollo de las nuevas tecnologías, las cuales han permeado en todos los ámbitos personales, sociales, políticos, profesionales, etcétera.

---

7 *Ibídem*, p. 27.

8 *Ibídem*, p. 28.

Es importante hacer una distinción en el ámbito del Derecho, pues ya que han surgido nuevas disciplinas, debido a la trascendencia de las tecnologías, por lo que hoy se conoce una nueva rama llamada Derecho de las Nuevas Tecnologías, la cual se define como: "el conjunto de normas y principios jurídicos que imponen deberes y confieren facultades que establecen la convivencia social de los fenómenos tecnológicos, cuyo fin es dotar a los miembros de la sociedad de los mínimos de seguridad, certeza, igualdad, libertad, justicia y competitividad"[9], en este sentido y debido a la utilización de las tecnologías han surgido conductas que pueden considerarse delictivas, dado que vulneran diversos bienes jurídicos, tutelados, sin embargo las cuales no se encuentran reguladas, que más adelante se abordaran, siendo una de las razones principales de esta rama, "el derecho de las nuevas tecnologías abarca la informática jurídica y el derecho informático".[10], lo cual pueden también considerarse ramas del derecho, incluso la informática jurídica una sub rama de cualquiera de las otras.

Para poder entender el derecho de las nuevas tecnologías, se deben conocer sus fines como la seguridad, la justicia y el bien común, en este sentido se puede entender como seguridad a "El ordenamiento del derecho de las nuevas tecnologías debe responder a la ineludible necesidad de un régimen jurídico estable, a la eliminación de cuanto signifique arbitrariedad. Importante contar con normas jurídicas bien determinadas y cumplimiento cabalmente garantizado"[11], en este sentido es primordial las normas jurídicas para la protección de los derechos y de los bienes jurídicos, que además se complementen con las políticas de prevención, en este caso de conductas que vulneren dichos derechos y bienes.

En segundo lugar, se encuentra la Justicia, la cual "Es la adaptación de la conducta del hombre a las exigencias de su naturaleza

9 Villanueva, Ernesto y Díaz, Vanessa, *op. cit*, p. 10
10 Ídem
11 Ídem

social. Según es la constante y perpetua voluntad de dar a cada uno lo suyo"[12], la justicia es la máxima del derecho, ya que a través de este último siempre se busca la justicia.

Por último, el bien común, que se refiere al "conjunto de valores, bienes y experiencias que contribuyen a la conservación y al progreso de la sociedad de la información y al bienestar materia, tecnológico, moral e intelectual de las personas que viven en ella"[13], como se sabe si bien es cierto el desarrollo de las tecnologías busca un bien común o satisfacer las necesidades del hombre, esto también ha lleva al surgimiento de algunas conductas que vulneran algunos derechos y bienes jurídicos, por lo que es necesario contar con una regulación para su protección.

III. LA POLÍTICA CRIMINAL Y SU TRATAMIENTO EN LOS DELITOS INFORMÁTICOS

En México es difícil hablar de conductas delictivas en materia de tecnologías, ya que, aunque el Código Penal Federal, hace mención de algunos delitos como, Revelación de secretos y acceso ilícito a sistemas y equipos de informática; Revelación de secretos y acceso ilícito a sistemas y equipos de informática o pornografía Infantil; así como algunos de los Códigos Penales de los Estados, entre los que destacan los códigos de la Ciudad de México y el de Nuevo León, no obstante lo anterior el hecho es en que han surgido un gran número de conductas en relación a el uso de las tecnologías, dichas conductas vulneran infinidad de bienes jurídicos tutelados, por lo que es necesario su regulación, más aun en las leyes penales federales y locales, por lo que es necesario partir de la Política Criminal.

Es importante conceptualizar la política criminal, toda vez que, conforme a sus fines generales como específicos, esta se basa en el bienestar de los ciudadanos y prevención de la delincuencia, tal y

12 Ídem
13 Ídem

como menciona Zúñiga Rodríguez en su libro "Política Criminal".

La Política Criminal refiere el Dr. Enrique Díaz-Aranda, es "exclusivamente al conjunto de decisiones políticas adoptadas por el Estado para luchar contra la criminalidad"[14], en este sentido refiere que parte de dos tipos de medidas las "informales y las formales"[15], las primeras son la "educación, la economía y la policía"[16], las segundas refieren a la "promulgación de nuevas leyes penales o a las reformas de las ya existentes"[17], además también refiere que la Política Criminal tiene tres principales funciones: histórica, la interpretación dogmática de la norma penal y la propuesta critica.

La función histórica principalmente tiene que ver con los antecedentes que dan pie a los legisladores a la creación de una norma penal, es decir en el caso de los delitos informáticos, serían el gran número de asuntos que han dado pauta a su posible regulación.

La función de la interpretación dogmática de la norma penal, se refiere principalmente si es que la norma ya se encuentra establecida, en no ir más allá de lo que plasmo el legislador, pues bien dice Díaz-Aranda, este es el "legitimo representante del pueblo"[18], en este caso tendría que existir penales sobre cada uno de los delitos informáticos que se conocen, para poder realizar una debida interpretación.

Por último la propuesta critica, la cual versa sobre los motivos que dieron origen a la norma y su posible funcionamiento, es decir se realizaría un análisis si es que esta función ultima cumpliría con la fines de la Política Criminal como son el bienestar social y la prevención de los delitos, esto a través de la prevención general negativa, específicamente el "temor a las leyes, no el temor a los

---

14 Díaz-Aranda, Enrique y Roxin, Claus, *Teoría del Delito Funcionalista,* Flores Editor, México, 2017, p.76.

15 *Ibíd.*

16 *Ibíd.*

17 *Ibíd.*

18 *Ibíd.*

hombres"[19], por lo que si se contara con los tipos penales de cada uno de los delitos informáticos, se tendría que analizar su posible funcionamiento en la prevención de dichas conductas.

Así mismo, también se puede referir a la Dogmática Penal, ya que "se ocupa de la interpretación, sistematización, elaboración y desarrollo de las disposiciones legales y opiniones de la doctrina científica en el campo del derecho penal"[20], esto implica indudablemente con la construcción de un tipo penal de cada uno de los delitos informáticos y todos sus efectos jurídicos que pudieran suscitarse, pues también la dogmática penal se encarga de "analizar al delito, el delincuente y la pena, desde el punto de vista normativo"[21].

Sería necesario una vez que existiera los tipos penales de cada delito informático, se tendría que analizar en el supuesto primero que nada a los elementos del delito o de la conducta, posteriormente a los delincuentes, que siempre quienes utilizan la tecnología como el medio principal para realizar una conducta, que sin la utilización de esta no se podría efectuar, y por ultimo las sanciones que surgieran de la misma; aunque cabe destacar que se tendría que realizar un análisis, de acuerdo al tipo de teoría con la cual se realice el tipo penal.

De igual forma, para una debida construcción de los tipos penales es necesario partir de las teorías, principalmente de la funcionalista, "que se apartan de la sistemática de la dogmática llamada "causalista""[22], probablemente se pensara que la más adecuada es la teoría funcionalista, ya que la política criminal busca que sea desde esta perspectiva, por lo anterior es necesario su análisis para una debida construcción del tipo penal.

---

19 Roxin, Claus, et. al., *Dogmática Penal y Política Criminal*, Flores Editor, México, 2015, p. 234.

20 Díaz-Aranda, Enrique y Roxin, Claus, *op. cit.,* p. 64.

21 *Ibídem,* p. 62.

22 Orellana Wiarco, Octavio Alberto, *Teoría del Delito,* Porrúa, México, 2005, p. 81.

La teoría funcionalista, se define como el "conjunto de hechos fisiológicos o de otra índole que se producen o suceden en un organismo, un aparato o un sistema"[23], por lo que se encarga principalmente al "estudio de las funciones dentro del sistema social concebido como una totalidad"[24], esta teoría funcionalista parte de dos corrientes el teleológico y el sistémico, cuyos exponentes son Claus Roxin y Günter Jakobs, cabe mencionar que la teoría funcionalista también parte de los mismos elementos del delito, sin embargo los toma desde una perspectiva de sistema y de la política criminal por lo que más adelante ya no se describirán dichos elementos, sino solamente se analizará desde que perspectiva lo toma la mencionada teoría.

Es importante recalcar que dentro de la teoría funcionalista y sus máximos exponentes existen el funcionalismo moderado de Claus Roxin, el "cual reconoce los elementos del delito propuestos por el finalismo (tipicidad, antijuridicidad, culpabilidad), pero con orientación político criminal"[25], por otro lado está el funcionalismo sociológico o radical de Günter Jakobs, el cual "considera al derecho como garante de la identidad normativa, la constitución y la sociedad, cuyo objeto es resolver los problemas del sistema social"[26], aun y cuando esta última se basa principalmente en el sistema social, ambas consideran en general los elementos del delito, como la acción, el tipo, la antijuridicidad y la culpabilidad enfocándose un poco más a la prevención de del delito desde la prevención general negativa a diferencia del finalismo.

Para Jakobs esta "se basa en la necesidad de entender el Derecho como parte un sistema social"[27], en este sentido prácticamente

23 *Ibídem,* p. 165

24 *Ibíd.*

25 Almanza Altamirano, Frank, *La Teoría del Delito, desde la Visión Finalista y Funcionalista*, Flores Editor, México, 2018, p. 22.

26 *Ibídem,* p. 27.

27 Alonso Ontiveros, Miguel, Derecho Penal, Parte General, INACIPE, UBIJUS, México, 2017, p. 115-116.

está hablando que el derecho es un estabilizador de dicho sistema, luego entonces quien dicho sistema "se encuentra en pautas de valor que definen expectativas del rol"[28], una vez que las personas no cumplen con su rol hay una "defraudación de expectativas"[29], para el funcionalismo el derecho penal va a fungir como un rector del comportamiento y no como protector de los bienes jurídicos tutelados, por lo que ocasiona que la persona "ceda toda su posición central de toda decisión penal al propio sistema"[30], por lo que prevalece el sistema.

Roxin "propone un sistema de Derecho Penal abierto capaz de recibir las valoraciones de sus conceptos y de sus principios por la vía político criminal"[31], esto contraviene lo establecido por la teoría finalista, pues la teoría funcionalista trata de asignarle una "función político-criminal"[32] a cada una de los elementos del delito, por ejemplo la acción, la tipicidad la antijuridicidad y la culpabilidad.

En el primer supuesto los que tengan al alcance un medio tecnológico y que por medio de este vulneren un bien jurídico tutelado, tendrían que funcionar conforme a su rol, entonces cuando incumplan con el mismo, a través de conductas sancionables por el derecho penal, desestabiliza al sistema cuyo fin es encontrar un equilibrio.

En cuanto al segundo punto en el caso de quienes utilicen las tecnologías y hagan un mal uso de ellas, habría que observarlos o más bien valorarlos bajo la política criminal a los elementos del tipo penal, una vez se construya los mismos.

Por otro lado, la teoría la acción se basa como "la exteriorización de la personalidad"[33], es decir que los actos desplegados o el comportamiento son el reflejo de la personalidad humana, en esta

---

28 Medina Peñaloza, Sergio J., *Teoría del Delito,* Ángel, México, 2003, p. 188.

29 Alonso Ontiveros, Miguel, *op. cit.,* p. 116.

30 *Ibíd.*

31 Medina Peñaloza, Sergio J, *op. cit.,* p. 194.

32 Alonso Ontiveros, Miguel, *op. cit.,* p. 114.

33 Medina Peñaloza, Sergio J, *op. cit.*, p. 196.

caso trata de cumplir con tres funciones, la clasificatoria, la coordinadora y la delimitadora, la primera tiene que ver con el "comportamiento delictivo (activo, omisivo, doloso, imprudente)"[34], cabe destacar bajo esta teoría se refiere que estos tienen que ver con los rasgos de la personalidad.

La función coordinadora y definitoria, contempla el hecho que la "exteriorización de la personalidad se vincula como concepto prejurídico"[35], y la función delimitadora de la acción, en la cual se excluyen supuestos, ya que si estos parten de la exteriorización de la personalidad, pero estos se ven modificados por algo ajeno a ellos, por lo que faltaría "la base anímica que conforma la identidad del sujeto"[36].

En la acción en los delitos informáticos, podría adecuarse por qué utilice las tecnologías como el medio principal para causar un daño a un tercero, se tendría que observar cómo se dio dicho menoscabo y posteriormente si es parte de su identidad.

La antijuridicidad, parte del hecho que funciona como "estabilización de expectativas que el subsistema jurídico desempeña dentro del sistema social"[37], esto es porque a través del cumplimiento de las expectativas jurídicas, se mantiene una estabilidad dentro del sistema.

En los delitos informáticos, se pueden como una expectativa sobre el actuar de quienes utilizan las tecnologías para un fin, sobre el que o no deben de realizar.

Por último la culpabilidad en la teoría funcionalista, se refiere a que "no puede justificar la pena más allá de las necesidades preventivas"[38], por lo que esta culpabilidad se liga principalmente a la acción, es decir quien exterioriza esa personalidad, se le puede

34 Íbidem, p.197
35 *Ibíd.*
36 *Ibíd.*
37 Íbidem, p.193
38 *Ibíd.*

exigir esa reprochabilidad, y el punto fin a la pena es la prevención.

En los delitos informáticos la culpabilidad obviamente, puede también adecuarse al que la pena vaya en caminada a una finalidad preventiva, que cause un impacto en aquel que utiliza de manera inadecuada las tecnologías.

IV. RELACIÓN DE LAS TIC CON EL SURGIMIENTO DE NUEVAS CONDUCTAS

Una vez analizada la teoría funcionalista y haber señala la importancia de una regulación en conductas que vulneran derechos y bienes jurídicos tutelados, es importante conocer cuáles son las conductas que han surgido con el uso de las tecnologías, las cuales:

Se reconocen como actos delictivos o potencialmente punibles a través de Internet, entre otros y de formas no exhaustiva, ni limitativa, los siguientes:

1. La difusión y la oferta de servicios sexuales y pornografía con participación de menores de edad (pedofilia y pornografía infantil).
2. La difusión de material obsceno o inmoral
3. La difusión de instrucciones sobre preparación de bombas, actividades terroristas, producción y tráfico de drogas, entre otras formas de discurso o información que atenta contra la seguridad.
4. La difusión de mensajes que incitan al odio y la discriminación sexual, étnica, racial, religiosa o de otro tipo.
5. La difusión de contenidos falsos que generen alarma o conmoción pública o inciten al desorden público.
6. La difusión de mensajes de calumnia, difamación o injuriantes.
7. Las conductas de hurto y destrucción de datos por parte de "hackers*, incluyendo información sensible de carácter privado o de seguridad nacional.
8. La recolección, procesamiento y transmisión no autorizada de datos de carácter personal.
9. La suplantación de identidad como ánimo de fraude, incluyendo la difusión de contenidos ilícitos haciéndose pasar por otro.

10. La difusión de información legalmente protegida, privilegiada o confidencial, tales como: secretos de carácter estatal, industrial o profesional.
11. La difusión no autorizada de contenidos protegidos por derechos de autor o derechos conexos. [39]

Estos son solo algunos ejemplos de algunas de las conductas que se han desarrollado con el uso de las tecnologías e incluso algunos ya se encuentran regulados como la pornografía infantil, sin embargo, hay más conductas que necesitan su regulación como el *phishing*, el secuestro de información, el *ciberbulling*, entre otros.

Las conductas que vulneran derechos y bienes jurídicos tutelados, no se pueden considerar delitos, toda vez que para ello se deben de encontrar tipificados, es por ello la importancia de su regulación, entonces se puede definir al delito informático como: "Toda aquella acción o conducta, típica, antijurídica y culpable, que consiste en el uso indebido de cualquier medio informático. La OCDE, lo define como cualquier conducta, no ética o no autorizada, que involucra el procesamiento automático y transmisión de datos"[40], en este sentido el uso de las tecnologías es el medio fundamental para la realización de este tipo de conductas, pues si bien es cierto que estas también han ayudado a otros delitos para su realización, como por ejemplo para el robo de identidad, el robo de autos con sistemas de seguridad mucho más complejos y cualquier otro que utilice a las tecnologías como herramienta, aunque no sea la principal o fundamental para llevar la conducta.

De acuerdo a lo anterior también han surgido nuevos conceptos como la criminalidad informática, la cual Ignacio Flores Prada, la define como "un género de delincuencia surgida al hilo del desarrollo de las TIC"[41], si bien es cierto que las TIC, es la mayor industria hoy en día, que además ha ayudado al desarrollo de otras más, así

39 García Barrera, Myrna Elia, *op. cit,* p. 561-562
40 *Ibídem*, p. 564
41 *Ibíd.*

como facilitado el quehacer humano en muchas de sus actividades, también es cierto que con ella se han desarrollado conductas que dañan los bienes jurídicos tutelados de las personas.

Como se ha mencionado la regulación de este tipo de conductas es de gran importancia, ya que son conductas que se desarrollan de manera muy habitual, por lo que diversos países han tomado acciones para regular dichas conductas, también en apego de diversos tratados, para ello la Organización de las Naciones Unidas, considera como delitos informáticos, los siguientes:

I. Fraudes cometidos mediante manipulación de computadoras.
   - Manipulación de datos de entrada
   - Manipulación de programas
   - Manipulación de datos de salida
   - Fraude efectuado por manipulación informática

II. Falsificaciones informáticas
   - Utilizando sistemas informáticos como objetos
   - Utilizando sistemas informáticos como instrumentos

III. Daños y modificaciones de programas o datos computarizados.
   - Sabotaje informático
   - Virus
   - Gusano
   - Bomba lógica o cronológica
   - Acceso no autorizado a sistemas o servicios
   - Piratas informáticos o hackers
   - Preproducción no autorizada de programas informáticos con producción legal.[42]

Esta clasificación, se realizó de manera genérica, sin embrago si realizara de manera específica, pudieran mencionarse por lo menos una decena más de delitos, los cuales requieren una regulación específica, a fin de que se contemplen todos los supuestos que se dan hoy en día.

Por mencionar solo algún ejemplo de las conductas que se realizan, como el robo intelectual, siendo uno de los más comunes ya que:

---

42 *Ibíd.*

> Además del aumento del número de incidentes de delitos cibernéticos, el robo intelectual habilitado cibernéticamente se ha generalizado en muchas partes del mundo. El nivel de sofisticación utilizado para robar propiedad intelectual hace que sea imposible evitar su atribución a un actor estatal. Algunos de los programas maliciosos que se han utilizado muestran signos de tener un origen regional y están diseñados específicamente para atacar ciertas zonas del mundo. Esta es una de las razones por las cuales la cooperación regional en la lucha contra el robo intelectual cibernético debería considerarse parte de un enfoque internacional y armonizado, dirigido por los Estados.[43]

Es por ello que en aras de la protección de la economía han surgido diversos acuerdos de cooperación internacional, con la finalidad de combatir este tipo de delitos, ya que hoy en día se dan de manera muy frecuente, incluso tratando de desestabilizar gobiernos o economías, a través de ataques informáticos a sistemas gubernamentales o bancarios.

En este sentido los daños ocasionados por este tipo de ataques *cibernéticos* han ocasionado grandes pérdidas económicas, pues:

> Se estima que los daños por delitos cibernéticos alcanzarán los US$6 billones para 2021, lo que equivale al producto interno bruto (PIB) de la tercera economía más grande del mundo. Además del costo financiero, el cibercrimen y los ciberataques socavan la confianza de los usuarios en la economía digital. Las encuestas indican que, de la población mundial con acceso a Internet, menos del 50% confía en que la tecnología mejorará sus vidas, lo que demuestra una creciente y profunda falta de confianza con respecto a la privacidad de los datos.[44]

Lejos de que la población confié en el desarrollo de las tecnologías y del uso del internet, como un recurso que mejoré la vida

---

43 Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe, recuperado en https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf, consultado el 20 de octubre de 2020.

44 *Ibíd.*

de estas, esto también debido a que no existen regulaciones para prevención y sanción de este tipo de conductas, lo que genera incertidumbre en los usuarios del as tecnologías.

El uso del internet como recurso que ha facilitado la comunicación entre las personas e incluso las actividades empresariales, gubernamentales, etcétera; también:

> Una de las características propias del internet es que no tiene fronteras; es decir, el ámbito geográfico es indeterminable, Esto tiene ventajas y desventajas, más en materia criminal representa una gran desventaja, pues genera problemas jurídicos sobre territorialidad, jurisdicción y competencia.[45]

En este caso por eso también es importante no solo la regulación a nivel nacional, sino, además es importante contar con tratados internacionales en materia de *cibercriminalidad* para facilitar la cooperación sobre competencia y jurisdicción. En este sentido, es posible la cooperación internacional a través de tratados en un ámbito universal o incluso regional, toda vez que se debe de considerar que:

> La naturaleza sin fronteras de los delitos que se perpetran en el ciberespacio, la cooperación regional en el desarrollo de capacidades es vital para poder reaccionar ante el crimen informático organizado y detener los ataques cibernéticos antes de que lleguen a niveles incontrolables. Los incidentes de ciberseguridad más recientes de 2017 y 2018 han demostrado el riesgo de un mayor daño financiero, y en términos de la cantidad de personas y Estados a los que afectan. Hemos sido testigos de operaciones de cibercrimen de enorme magnitud, que han detenido el desarrollo normal de las economías nacionales, teniendo como objetivo específico algunos de los pilares centrales de las economías de los Estados, como los sectores industrial y bancario. [46]

---

45 Villanueva Ernesto y Díaz Vanessa, *op, cit*, p. 79

46 Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe, *op. cit.* p. 35

Como se mencionó anteriormente es importante la cooperación internacional en reacción a este tipo de conductas, pues tan solo en México en los últimos 5 años, han surgido una gran cantidad de ataques *cibernéticos* al sistema bancario, lo que ha causado una gran pérdida de recursos para dicho sector y para los particulares usuarios de los bancos que han sufrido los ataques.

Es por ello que además de la necesaria regulación de dichas conductas, también es necesario políticas de prevención o der *ciberseguridad*, las cuales:

> Son fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como la privacidad, la propiedad, así como para aumentar la confianza de los ciudadanos en las tecnologías digitales, y que éstos puedan sentirse cómodos accediendo a dichas tecnologías. El crimen en línea ya supone, aproximadamente, la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo. A nivel agregado, las cifras adquieren aún mayor magnitud pues los daños económicos de los ataques cibernéticos podrían sobrepasar el 1% del producto interno bruto (PIB) en algunos países. En el caso de los ataques a la infraestructura crítica, esta cifra podría alcanzar hasta el 6% del PIB.[47]

Por lo que es necesario la regulación y las políticas necesarias para prevenir y sancionar este tipo de conductas, mientras no existan este tipo de medidas, no se podrá generar confianza en los usuarios para que utilicen de manera habitual, libre y segura las tecnologías como un medio para facilitar sus actividades.

V. RETOS

Hay muchos retos sobre el Derecho de las Nuevas Tecnologías frente a las diferentes conductas y actividades que se realizan con el uso de las tecnologías, en este sentido uno de los principales retos es la regulación, en este sentido:

47 *Ibíd.*

> La base para la investigación y procesamiento del ciberdelito es una legislación adecuada, que incluso ayude a prevenir la comisión de este tipo de conductas delictivas ilícitas. sin embargo, los legisladores deben responder constantemente a los desarrollos de internet y supervisar la eficiencia de las disposiciones existentes, especialmente teniendo en cuenta la velocidad del desarrollo de las tecnologías de redes. [48]

Pero no solo el reto de una necesaria regulación es un problema, pues principalmente el sector político y legislativo no cuenta con los conocimientos técnicos para poder plantear políticas y a su vez propuestas para una posible regulación de estas conductas, además que los avances tecnológicos y las conductas delictivas que surgen de estos crecen de manera exponencial, sin que se estén preparados para ello.

Además, también existen otro tipo de retos, principalmente en el ámbito jurídico penal, ya que:

> El retraso existente entre el reconocimiento de abusos potenciales de las nuevas tecnologías y las modificaciones necesarias que deben introducirse en las leyes penales nacionales. Este reto sigue siendo tan importante y fundamental puesto que cada vez es mayor la velocidad en la innovación de las redes y de las tecnologías de la información y comunicación. [49]

En este sentido es importante señalar que los avances en las tecnologías de la información y comunicación son exponenciales, lo cual trae consigo nuevas conductas al mismo tiempo de la actualización de las tecnologías, por lo que es evidente que debe existir una regulación para la prevención y la sanción de las mismas, en este caso desde el derecho penal, hablando de lo que hoy se conoce como *ciberdelitos* y aunque como se ha mencionado existen decenas de este tipo de delitos, su tratamiento jurídico mayormente se ha

---

48 Villanueva Ernesto y Díaz Vanessa, *op. cit.* p. 80

49 *Ibíd.*

realizado en instrumentos internacionales y no así en el ámbito federal y local, por lo que "la legislación contra el ciberdelito debe ser parte integrante de una estrategia de Ciberseguridad"[50], por lo menos para afrontar los problemas delictivos en dicha área en nuestro país y estar en concordancia con los instrumentos internacionales.

Además, se debe de plantear una Política Criminal encaminada a los llamados *ciberdelitos* o delitos informáticos, con el fin de dar un bienestar de los ciudadanos y prevenir la delincuencia, además como refiere el autor Enrique Díaz Arana, la política criminal se refiere "al conjunto de decisiones políticas adoptadas por el Estado para luchar contra la criminalidad"[51] en este caso a la *cibercriminalidad,* tal vez se piense que este término no es necesario, sin embargo con el desarrollo e inmersión de la tecnología en prácticamente cualquier actividad humana, es totalmente valido hablar de *cibercriminalidad,* como objeto de la Política Criminal.

Es importante hablar sobre *cibercriminalidad*, toda vez que, debido a la interacción humana y la tecnología, cualquiera puede ser susceptible a ser víctima de un *ciberdelito* o delito informático, para afrontar dichas conductas es necesario como ya se comentó partir de una Política Criminal con enfoque de *ciberseguridad* y la debida regulación en las leyes penales, para ello se necesitan:

> Los esfuerzos para hacerlo deben ser de naturaleza multidimensional, porque se requiere una variedad de factores para construir una cibersociedad resistente. Las políticas y los marcos legales deben ajustarse y todas las partes interesadas de la sociedad civil, así como los sectores público y privado, deben trabajar para crear una cultura de ciberconciencia y capacitar a profesionales calificados para construir una estrategia de ciberseguridad; por lo tanto, es un esfuerzo continuo y complejo.[52]

---

50 *Ibíd.*

51 Díaz-Aranda, Enrique y Roxin, Claus, *op. cit*, p.76.

52 Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe, *op. cit.* p. 12

El crear una conciencia en la población, en el sector público y privado sobre los *ciberdelitos* es algo muy complejo; lo anterior ya que lo primero que se tiene que hacer es que el sector público, cree políticas públicas o política criminal/*cibercriminal* sobre el uso de las tecnologías para concientizar a los usuarios; así mismo involucrar a través de estas políticas al sector privado para mejorar sus sistemas informáticos; y por ultimo difundir con los usuarios y esto solo es una pequeña parte de las acciones a realizar, toda vez que se tiene que abordar el aspecto legislativo para tipificar todas aquellas conductas que se están suscitando, aunque esto último requiere un estudio más profundo de especialistas en dichas áreas.

Sin embargo, es donde vienen los retos para el país, ya que al ser un país subdesarrollado no cuenta con la infraestructura ni el conocimiento necesario para afrontar dicha problemática, en este sentido:

> Centroamérica y México, ambos presentaron un nivel de madurez promedio de 2 en las dimensiones "Cultura y sociedad" y "Educación, capacitación y habilidades", mientras que en las dimensiones "Política y estrategia" y "Estándares, organizaciones y tecnologías" el puntaje ha sido inferior a 2. Al igual que en el Grupo Andino, Centroamérica y México deberían centrarse en mejorar el despliegue de estándares de seguridad cibernética y controles técnicos, así como fomentar el desarrollo de un mercado de ciberseguridad. Cabe destacar que la dimensión "Marcos legales y regulatorios" tiene un nivel de madurez de entre 2 y 3. México presenta la mejor posición de la región, con un nivel de madurez de entre 2 y 3 en casi todas las dimensiones[53]

Aun y cuando México, es uno de los mejores evaluados en América Latina y el Caribe, es importante poder acercarse a las condiciones como países europeos e incluso de Norteamérica, lo anterior ya que "dada la naturaleza global de la amenaza, la construcción y preservación de alianzas y asociaciones sólidas con terceros

53 *Ibíd.*

países es fundamental para la prevención y disuasión de los ataques *cibernéticos*, que son cada vez más trascendentales para la estabilidad y la seguridad internacional"[54], lo anterior ya que la mayoría de los ataques *ciberneticos* a gran escala son en contra de empresas internacionales y a los diferentes gobiernos, lo que perjudica indirectamente a la población, en este mismo sentido, cabe mencionar que la mayoría de los *ciberdelitos* o delitos informáticos son cometidos en contra de los particulares, por lo que se necesita de la cooperación Internacional para buscar disminuir se cometan este tipo de actividades y se fomente la regulación en los diferentes países, en este caso ya que:

> Los cibercriminales aprovechan rápidamente los nuevos vectores de ataque y se benefician de los vacíos en la cooperación de las fuerzas del orden público en las diferentes jurisdicciones, dada la naturaleza inherentemente transnacional de sus actividades maliciosas. A su vez, el riesgo de ataques cibernéticos en infraestructura crítica y fraude o robo de datos ha sido siempre una prioridad para los líderes empresariales a nivel mundial.[55]

Como se mencionó anteriormente los ataques *cibernéticos* a las empresas internacionales, sea de manera directa o indirecta, terminan perjudicando a los particulares, por lo que es importante existan ordenamientos normativos a nivel universal, regional, federal y local, así como mecanismos para su prevención en los mismos niveles. Más aun cuando el dinamismo en las tecnologías requiere que la normatividad y los mecanismos sean igual de dinámicos, ya que "la naturaleza de los actos criminales que tienen lugar en el ciberespacio está cambiando rápidamente, por lo que los países deben invertir más en educar a su personal en la aplicación de la ley, los sistemas judiciales y otras instituciones gubernamentales relevantes"[56], en este caso basados en Política criminal o *cibercriminal.*

54 *Ibíd.*
55 *Ibíd.*
56 *Ibíd.*

VI. CONCLUSIONES.

Indudablemente es necesario una regulación en materia de *ciberdelitos* o delitos informáticos, en relación a las diversas conductas que han surgido del uso de las tecnologías ya que estos de manera particular vulneran los bienes jurídicos tutelados por las normas jurídicas, por lo que se debe comenzar desde una Política Criminal/ *Cibercriminal*, ya que las decisiones del sector político deben de estar encaminadas a disminuir dichas conductas, mediante la regulación jurídica en las normas penales en cuanto a su tipificación de dichas conductas, y cumplir con el cometido de estas políticas que es la lucha contra la criminalidad, lo cual debe de ir en concordancia con los instrumentos internacionales en *ciberseguridad*, así como fortalecer la cooperación internacional entre los estados para crear nuevos instrumentos y mecanismos que ayuden a prevenir y sancionar este tipo de conductas delictivas.

En este mismo sentido deben de realizar políticas encaminadas a la creación de conciencia entre los usuarios de las tecnologías, así como el apoyo de los especialistas en seguridad informática y en Derecho de las Nuevas Tecnologías, hacia las grandes corporaciones y gobiernos que son los principales afectados por la *cibercriminalidad*, que deben de encargarse de la creación de políticas y mecanismos de *ciberseguridad* que ayuden a reducir y sancionar los *ciberdelitos* o delitos informáticos.

VII. FUENTES DE CONSULTA.

Bibliografía

Almanza Altamirano, Frank, La Teoría del Delito, desde la Visión Finalista y Funcionalista, Flores Editor, México, 2018.

Alonso Ontiveros, Miguel, Derecho Penal, Parte General, INACIPE, UBIJUS, México, 2017.

Arellano García, Carlos, Métodos y Técnicas de la Investigación Jurídica, Porrúa, México, 2018.

Díaz- Aranda, Enrique y Roxin, Claus, Teoría del Caso y del Delito en el Proceso Penal Acusatorio, STRAF, México, 2015.

Díaz- Aranda, Enrique y Roxin, Claus, Teoría del Delito Funcionalista, Flores Editor, México, 2017.

Flores Salgado, Lucerito, Derecho Informático, Grupo Editorial Patria, México, 2013.

García Barrera, Myrna Elia, Derecho de las Nuevas Tecnologías, UNAM, Instituto de Investigaciones Jurídicas, México, 2011.

García Barrera, Myrna Elia, Manual de Derecho de las Nuevas Tecnologías, Tirant lo Blanch, México, 2018.

López Betancourt, Eduardo, Teoría del Delito y de la Ley Penal, Porrúa, México, 2015.

López Medrano, Delio Dante, Derecho Penal. Parte General, Flores Editor, México, 2018.

Medina Peñaloza, Sergio J., Teoría del Delito, Angel, México, 2003.

Muñoz Conde, Francisco, Teoría General del Delito, Tirant lo Blanch, Valencia, 2007.

Orellana Wiarco, Octavio Alberto, Teoría del Delito, Porrúa, México, 2005.

Roxin, Claus, et. al., Dogmática Penal y Política Criminal, Flores Editor, México, 2015.

Téllez Valdez, Julio, Derecho Informático, McGraw-Hill, México, 2009.

Villanueva, Ernesto y Díaz, Vanessa, Derecho de las Nuevas Tecnologías, Oxford, México, 2015.

CIBERGRAFÍA

Zambrano Martínez, Fernando, Las TICS en nuestro ámbito social, recuperado en: http://www.revista.unam.mx/vol.10/num11/art79/int79.htm, consultado el 20 de mayo de 2020.

Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe, recuperado en https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf, consultado el 20 de octubre de 2020.

NADA NUEVO ES QUE NOS VIGILEN. EL USO DE DRONES Y SU REGULACIÓN

José Antonio Alvarez León*
Vianey Vega Maldonado**

SUMARIO: I. Introducción. II. Drones una aproximación desde la Política Criminal. III. Evolución y Tecnología de los Drones. IV. Perspectiva Constructiva en el Uso de Drones V. Utilización de Naves no Tripuladas, por Razones de Seguridad Nacional y Orden Público VI. Normatividad que Regula el Uso de Aeronaves no Tripuladas en México. VII. Reglamentación internacional Como Referente en el Uso de Tecnología Dron.

I. INTRODUCCIÓN

Dentro de la política criminal ya sea en su definición amplia en el contexto político-jurídico del discurso de control del delito o la definición restringida y operativa de las prácticas institucionales para cumplir fines preventivos respecto de las acciones criminales, el tópico respecto de los usos tecnológicos se vuelve inevitable, pues la vida del hombre posmoderno discurre en tres planos, el físico, el cibernético y en la combinación de ambos, lo que le permite al individuo realzar acciones múltiples actividades conectadas o aisladas unas de otras pero con afectación directa en su modus de vida.

De esta forma el crimen y las amenazas a la seguridad de la nación se ven presentes en diferentes planos y para combatirlas o anticiparse a ellas la vigilancia oculta se vuelve una necesidad imperiosa. Los drones, son un parte de esa tecnología de control y prevención. Su uso justificado desde el discurso del poder del Estado

* José Antonio Alvarez León. Profesor investigador en el departamento de Posgrado en Derecho y Política Criminal. Fes Acatlán UNAM.

** Licenciada en Derecho y Estudiante de la Maestría en Política Criminal en la UNAM, FES Acatlán.

está justificado en el contexto de la prevención con límites legales y su uso armado con fines militares sin embargo, existe una línea muy endeble donde la ética policial deberá de ser el eje conductor para que la vigilancia no sea espionaje de adversarios o para extorsionar personas inocentes o los usos militares no sirvan para la represión o la eliminación selectiva.

Bajo estos parámetros, la idea central de este artículo es explicar y reflexionar que son los drones, su uso técnico legal y que puede advertirse al respecto de ellos desde el campo de la política criminal y punitiva de estado mexicano.

Se trata de advertir como esta herramienta tecnológica, puede ser beneficiosas a la luz del servicio que dará en el sentido de lo público, pero también a la mirada de alerta ante los usos de invasión permanente de los espacios privados. Los drones, pueden a decir de *Bauman*, ser ese panóptico permanente donde delincuentes e incautos pueden ser vigilados desde dentro de sus propios resguardos privados.

II. DRONES UNA APROXIMACIÓN DESDE LA POLÍTICA CRIMINAL.

Nada nuevo es que nos vigilen. Desde tiempos inmemoriales para los grupos dominantes en las sociedades o en los Estados modernos vigilarnos ha sido una prioridad, siempre, todo el tiempo y mientras más sepan de nosotros (sociedad), será mejor para ellos. Vigilar a la sociedad ha tenido como fin prioritario prever cualquier intento por usurpar el poder, por esto, anticipar todo lo necesario para desvanecer cualquier liderazgo, por manipular la información que pueda generar apertura de las mentes dóciles o incautas ha sido y será siempre una prioridad, para las cúpulas del orden social.

Vigilar, también es una práctica que fue dando sus frutos en los espacios privados, bajo los mismos argumentos (control y poder) pero en sistemas diferentes, por ejemplo, en las empresas, los negocios e incluso en los ámbitos más sencillos como en las reuniones de trabajo o las conversaciones privadas.

Quienes controlaban y controlan, antes y ahora, necesitan de ojos, odios en todas partes. Los medios han variado y la información que han obtenido también ha cambiado, pero la práctica se ha vuelto fructífera. Evidentemente cuando alguien nos vigila o vigila algún lugar se produce un espacio de vulnerabilidad, de entrega sin consentir y por supuesto, se comenten otros ilícitos además de entrar a nuestra intimidad. Observarnos de forma oculta (espiar), es vulnerar a otros qué tienen relación con quienes son el blanco específico o con los que se comparte el lugar, es por ello que espiar tiene sus matices, por muy vulgar, poderosa o legal que sea esta práctica.

Los matices del espiar cambian en función del momento histórico, de la persona que lo haga, del medio usado y por supuesto, de los fines. Espiar-vigilar nos puede situar en un conflicto discursivo y ético, que en el menor de los casos dependerá, de cómo y cuándo se usa la información o las imágenes obtenidas. Estando entonces lejos del debate moral o de trastrocamiento de la libertad y el derecho a la intimidad hoy, esta práctica la centraremos únicamente en el contexto de los beneficios o daños.

Cuando se habla de los daños, necesariamente nos situamos en las actividades que se pueden causar como; chantajes inmorales y una diversidad de delitos. La actividad delincuencial sabe bien que su protección dependerá del factor anticipación a ciertas acciones policiales y de sus enemigos, pero también a la sorpresa sobre la víctima. En la era global, espiar para cometer un ilícito o generar terrorismo es muy común y requiere de tecnología. Para realizar esas actividades se requiere burlar la ley, sembrar miedo y demostrar poder, por eso, tener la información de las victimas requerirá de un trabajo permanente sobre las tecnologías como armas para cometer sus fines lesivos "La anarquía global y la violencia se nutren mutuamente, se refuerzan y se dan ímpetu la una a la otra; como la vieja máxima nos advierte inter arma silent leges..." (Sic). Vigilar, es y será una ventaja para el delincuente porque une espacios físicos y virtuales "los retos de la seguridad en el mundo

analógico se incrementan. En este sentido el uso de drones para actividades delictivas va de ser usados para entregar drogas y celulares dentro de reclusorios, hasta el robo de datos a través de redes," La tecnología de drones, telefónica y radiofónica no son costosas para la delincuencia organizada y trasnacional, y de serlo, para ellos es altamente redituable.

Los delitos más comunes ejecutados bajo la tecnología de drones son: Espionaje de intimidad, seguimiento de personas, revisión de espacios, vigilancia "Halcones" acoso, entrega de objetos en reclusorios (drogas, aparatos de comunicación), terrorismo, robo de información virtual, daño de torres y medios de comunicación, registro de operaciones policiales, violación de espacios aéreo privado, obtención de imagines de personas adultas y menores para usos ilícitos, etc.

Los delincuentes cambian sus modos de operación y sus zonas de trabajo tan rápido como la sociedad lo hace por lo que su adaptabilidad siempre es más veloz y fructífera que incluso la de los cuerpos de seguridad. La relatividad de los delitos en mucho dependen de su cambio permanente y ágil, pero en el caso de las tecnologías haciendo bivalente los delitos es decir, que se comete físicamente como se describe en la ley (objeto del ilícito) y se dan sólo cambiando el modo descrito en la misma, por el cambio en el medio comisivo y la forma de actuación, lo que permite no sólo innovar en la ejecución sino en caso de ser detenido, burlar la ley, pues no habría encuadramiento típico idóneo. Además, el delito ejecutado físicamente también se comete a la par través de medios electrónicos generando una fragmentación del delito, pues dicha combinación puede implicar traer victimas del mundo virtual al físico o tener víctimas en ambos espacios al mismo tiempo.

Los beneficios. El uso de los drones y la tecnología vistos desde los aparatos de control del Estado se van enmarcando en dos sentidos, los que a plena luz podemos encontrar en las disposiciones legales y en que se da en práctica de las fuerzas del orden más allá

del aspecto legal. Sin embargo se pueden dar ambas formas en una solo práctica.

La guerra fría desató la carrera tecnológica armamentista en los 70´s y 80´s pero el triunfo de occidente disparó los conflictos asimétricos haciendo que la tecnología fuese la estrategia de combate, por ejemplo contra el mundo musulmán y el terrorismo. Se buscó la lucha a distancia y la geolocalización como herramienta para detectar al enemigo, sin embargo el dron evolucionó para ser no sólo un arma de vigilancia sino de también de eliminación "lo que es nuevo es el dron, acertadamente llamado *Predator*, que ha asumido la función de reunir y procesar información… la función manifiesta de un dron, es permitir al operador localizar el objetivo de ejecución", así, este nuevo aparato tecnológico se volvió clave para desarrollo legal de las fuerzas armadas no tripuladas .

Como suele pasar con la tecnología, el dron ha pasado al ámbito civil con gran velocidad cambiando limitando sus usos a los de rastreo, vigilancia y por supuesto espionaje.

En el ámbito policial esta tecnología se ha ido usando como una práctica cotidiana, y con ella se reafirma la intención del Estado de mantener el control tecnificado. Sin embargo, la actualización técnica de la policía está ajustada a estrategias de política criminal institucional es decir, es vista como un medio para combatir el delito y el control penitenciario sin modificar ningún planteamiento sustantivo como el fundamento del derecho penal y los derechos humanos como políticas de Estado (al menos en México), por tanto el uso de la tecnología es parte de quehacer operativo de la institución.

La tecnificación policial tiene un sentido ético general desde el cual se obliga a los operadores de la seguridad a actuar conforme a sus reglamentos basados en la ley constitucional, por tanto el dron y otros medios tecnológicos cumplirían su fin de forma segura; sin embargo, la pregunta clave seria ¿en el Estado de Derecho existen espacios donde el actuar policial sea invisible? con el fin de anticipar acciones de para el control efectivo, la respuesta es afirmativa.

La tecnología permite que desde el anonimato o el ocultamiento, la policía u otros cuerpos represores del Estado, puedan mirar todo el tiempo a sus seleccionados por ser catalogados como criminales, ser enemigos políticos o peligrosos. Un dron, a diferencia de un satélite, perite cercanía, precisión, rastreo, perfeccionamiento sobre su blanco e incluso, escucha y vigilancia dentro de lugares donde el satélite no puede llegar "Los drones pueden ser tan pequeños como un colibrí, pero el néctar que buscan son imágenes de alta resolución…" Nada nuevo es entonces que los cuerpos de seguridad puedan estar en todos lados a toda hora, al menos desde la voluntad de seguir a alguien o mirar a través de ciertos espacios; es como hacer realidad la predicción de *Orwell* donde porque el dron como otros instrumentos tecnológicos develaran en su uso quienes somos, dónde estamos, con quién convivimos, por donde nos movemos, el gran hermano sabrá todo con tan solo esperar a que usemos la tecnología o que él, la use sobre nosotros.

El dron sin embargo, prever en acciones policiacas enfrentamientos violentos, permite que es vigilancia fuera de ley (no sea prueba en un proceso) sirva para seguir y combatir a los criminales y en ello estribaría nuestra seguridad.

Hoy las políticas públicas de vigilancia y las acciones del Estado con uso militar o policial, estan revestidos de un auto control ético , pues como ya se dijo, difícilmente el ciudadano promedio sabrá cuando es visto a lo lejos y por cuanto tiempo. Al final debemos recordar que en un mundo caótico donde las dimensiones del orden son difusas los criterios de control de la política criminal están por mucho doblemente cedidos por la ciudadanía, primero, por la disposición legal (por nuestros derechos límites al actuar punitivo del Estado), segundo, por la voluntad propia para que autoridad hago algo que no sería legal (salvo por nuestra permisión), pero permitimos que lo haga en nuestro espacio privado por sentirnos seguros (renuncia a nuestras libertades), nos referimos al permitir que la autoridad nos registre y controle para sentirnos más seguros al saber

que lo hace también con otros o nos confinamos al encierro por sentirnos no asilados sino protegidos dimensionando así nuevas formas de la vida comunitaria "la vigilancia y las acciones defensivo/agresivas que desencadenan crean un propio objeto. Gracias a ellas el extraño es trasmutado, en algo ajeno y lo ajeno en amenaza (…) "comunidad segura" es la extraña mutación a un gueto voluntario" La vigilancia a distancia, puede es una herramienta de matices, porque también puede generar auto vigilancia de las acciones policiales pudiendo distinguir con ello si se actuó en determinadas circunstancias conforme a derecho, por tanto un dron se vuelve una herramienta de matices.

El uso de la tecnología en las políticas de control del delito, tendrán que ser bienvenidas porque ellos conlleva a un derecho penal científico, donde la seguridad de los hechos que se controlan y se ponen en la mesa de los juzgados deberán de atender siempre a hechos comprobables, en virtud de que los usos técnicos y científicos permiten la contra prueba y la validación de lo que se esgrime desde ellos. Desde el ámbito de la seguridad pública el anonimato u ocultamiento de la vigilancia quedará sujeto a la llamada investigación no controlada (son conocimiento del juez) en cuento no se afecten derechos de terceros o no se usen las imágenes captadas son un contexto de imputación formal, porque de otra forma la ventaja siempre será del criminal.

La vigilancia por drones se ubica dentro de la política criminal en la parte del análisis discursivo y después en la parte preventiva, esto es así porque referimos a dimensiones de poder. La vigilancia tecnificada y oculta con efectos represivos reales a nivel institucional es sin duda alguna un expresión de poder autoritario ejercido por el estado de derecho (porque pude usarse para aniquilar adversarios o violar derechos de las personas), por tanto el poder como expresión de control de las voluntades conscientes o no, significan la idea de saber todo, todo el tiempo y dominar las fuerzas (de la naturaleza que sean en sentido social) que buscan desestabilizar el

sistema jurídico-político; por tanto, hablamos de poder oculto cuyo fin debe interpretarse como acción para evitar problemas, aún bajo los riesgos de uso faccioso.

Por otro lado y como ya se dijo, la vigilancia oculta por drones significa atajar las acciones criminales y establece con imágenes y sonidos, evidencia de actividad criminal o de riesgo a la seguridad nacional. En este sentido será necesario conocer y contextualizar de forma precisa el uso y regulación de los drones como se hará en los puntos siguientes.

III. EVOLUCIÓN Y TECNOLOGÍA DE LOS DRONES

Es importante tener mayores implicaciones en los avances tecnológicos, y conocer los aportes que estos pueden tener en la elaboración de políticas públicas y políticas criminales acorde a la tendiente evolución de la sociedad y de los grupos criminales.

En este rubro de elementos tecnológicos se atiende al uso que a través del tiempo han tenido los sistemas de Aeronaves Pilotadas a distancia (SAPD), por su nombre en inglés *Remotely Piloted Aircraft* (RPAS), *unmanned Aircraft Vehicle* (UAV), *unmenned Aerial Systems* (UAS), popularmente conocidos como DRONES[1], cuyo enfoque comenzó direccionado únicamente al ámbito militar y paulatinamente fue diversificándose hasta llegar a ser asequible para cualquier ciudadano.

Los primeros antecedentes de los RPAS se remontan al año 1849 cuando en Austria fueron lanzados 200 globos sin piloto cargados con bombas con el objetivo de bombardear Venecia, Italia[2], luego la invención del control a distancia por parte de Nikola Tesla en diciembre de 1898, vino a complementar los primeros intentos de pilotar una aeronave a distancia.

---

1 La palabra DRON proviene del inglés *DRONE* cuyo significado original era zángano (macho de la abeja reina) y luego se aplicó a aeronaves no tripuladas por su zumbido. http://etimologias.dechile.net/?dron#:~:text=La%20palabra%20dron%20(avi%C3%B3n%20o,no%20tripuladas%2C%20por%20su%20zumbido. Consultado 18 nov 20

2 López Velarde Samuel Chacón, *Los Drones y su Legislación en México,* Ciudad de México, Tirant lo Blanch, 2017, p. 17,18.

Hacia el año 1917 Elmer Sperry y Peter Tlewitt construyeron el primer aeroplano de radiocontrol "*Hewitt-Sperry Automatic Airplane*" (bomba voladora o "flying bomba") con capacidad de vuelo cargada de explosivos, cuya fuente de vuelo era una catapulta neumática; bajo ese esquema el ejército Estadounidense mejoro el diseño, la fuente de lanzamiento era ya un torpedo lanzado sobre vías o rieles, resultando la fabricación del Kettening Aerial torpedo "*Bug"*, peculiar en virtud de que después de cierto tiempo, vía remota se apagaba y se le desplegaban alas para redireccionarlo hacia algún objetivo en donde la carga explosiva que portaba era detonada a su impacto con la tierra.

En Alemania durante la primera guerra mundial (1915-1918) la utilización de los SAPD era bajo el diseño de un misil lanzado desde un globo aerostático y después guiado vía radio control; su desarrollo eficaz se materializo en la segunda guerra mundial cuando su uso se centró en el ámbito militar como misiles manejados por radio control, incluso algunos emitían señal de tv para lo cual contaban con cámaras de transmisión. El empleo de dicha tecnología obedecía a que los SAPD eran más seguros y rentables lo cual reducía el número de aeronaves tripuladas derribadas y pilotos muertos.

De este modo la versatilidad de usos de los SAPD fue evolucionando al incursionar en misiones de espionaje y vigilancia, incrementándose en la guerra fría, ya en la guerra de Vietnam el uso principal de los drones fue para reconocimiento de tierra y vigilancia.

En las décadas de los 70´s y 80´s el desarrollo tecnológico de los sistemas de posicionamiento global o *Global Positioning System* (GPS), de las computadoras, del equipo y componentes livianos y controles de vuelo digitales y comunicación satelital, fue incorporado en la fabricación de los SAPD dando como resultado sistemas aéreos teledirigidos de la más alta calidad, de entre los que destacan los

modelos ALBATRON[3] y AMBER.

Ante la rentabilidad y eficiencia de la tecnología dron su desarrollo y transformación sigue avanzando, diversificándose su uso en los ámbitos militar, comercial, recreativo, seguridad nacional, seguridad pública, entre otros.

IV . PERSPECTIVA CONSTRUCTIVA EN EL USO DE DRONES.

El uso de la tecnología dron se está convirtiendo en un tendencia, popularizándose su empleo multipropósito en virtud de la reducción de costos, tiempo y la facilidad de acceder a ella, su utilización es tanto en actividades meramente recreativas como la fotografía, deporte, competencias, juegos, etc. hasta en actividades especializadas como: estrategias militares, de aduanas, de policía, de búsqueda y salvamento, control de fronteras, vigilancia costera o similares, investigación de una escena del crimen, incluso hasta como medio de transporte de armas y sustancias peligrosas.

También en actividades agroforestales y enfocadas a la preservación del medio ambiente; como son la prevención y control de incendios, parametrización del índice de contaminación lumínica, control y seguimiento de accidentes industriales con vertidos tóxicos en medios acuáticos, realización de mapas geológicos, visualización de movimientos de tierras, determinación y control a escala centimetrica de áreas de riesgos geológicos, etc. Así también en actividades de investigación científica y desarrollo, tales como análisis de cartografía, empleo en el rubro de la construcción, control y análisis de multitudes, entre otras.

En otras palabras desde una perspectiva constructiva, el uso de RPAS aporta ventajas e importantes beneficios incluso más allá de

3 Albatross fue lanzado en el 2014 como primer modelo de dron con altas capacidades de vuelo y carga, diseñado para múltiples actividades como la conservación de vida marina, ayuda humanitaria, investigación, vigilancia, operaciones comerciales y actividades técnicas. https://www.appliedaeronautics.com/albatross-uav consultada 18 -11- 2020

la rentabilidad, facilidad y eficacia de resolución de problemas, lo es la posibilidad de emplearlos con la finalidad de salvar vidas humanas; sin embargo, a la par se debe ser sensible a la transgresión de derechos fundamentales que su uso conlleva y de los riesgos que por la naturaleza de sus funciones representa como son los riesgos de accidentes, el acceso que los delincuentes tienen a esta tecnología y el más preocupante para el común de la gente que es la vulnerabilidad de su privacidad en las acciones de vigilancia furtiva.

V. UTILIZACIÓN DE AERONAVES NO TRIPULADAS, POR RAZONES DE SEGURIDAD NACIONAL Y ORDEN PÚBLICO.

Las acciones de gobierno en las que se ha visualizado la utilización de los RPAS han sido tendientes a preservar la seguridad nacional y el orden público, para generar un contexto a lo anterior se aduce importante comprender los alcances de la Seguridad Nacional en donde el uso de drones ha contribuido activamente, así como la necesidad de regulación para incidir en que su uso contribuya a preservar el orden público.

El derecho a la Seguridad Nacional se generó con la reforma constitucional de 2004, que dio paso a la publicación de la Ley de Seguridad Nacional el 31 de enero de 2005 en el Diario Oficial de la Federación, ordenamiento legal que concede la facultad y obligación al Titular del Ejecutivo Federal de preservar la Seguridad Nacional, con la colaboración de las autoridades federales, de las entidades federativas y de los municipios.

Al respecto se asume sin lugar a duda que la delincuencia organizada ha constituido un flagelo y una de las amenazas que durante años a puesto en riesgo a nuestro país, en especial la generada por el narcotráfico y robo de hidrocarburos, bajo ese contexto, dentro de las acciones destinadas a mantener la integridad, estabilidad y permanencia del Estado mexicano, la Secretaria de la Defensa Nacional, se ha visto en la necesidad de desarrollar operaciones contra el narcotráfico, vigilancia de instalaciones estratégicas y de

zonas fronterizas y protección a la población civil (apoyo al Plan DN-III-E).

De modo que, por conducto de la Fuerza Aérea Mexicana, la SEDENA tuvo a bien iniciar gestiones en junio de 2008 para adquirir un sistema de aviones no tripulados "HERMES 450" de fabricación Israelita, para cuya operación fue creado el Escuadrón de Sistemas Aéreos no tripulados (ESANT) iniciando actividades en julio de 2009, mediante el análisis y planeación de operaciones desde un centro de control remoto.

La SEDENA ha puesto especial interés en el uso de RPAS, incluso dentro del programa sectorial de defensa Nacional 2012-2018 se estableció que el indicador estratégico relativo a la inversión de aeronaves no tripuladas debía tener continuidad, ya que si bien es cierto para la adquisición de tres sistemas aéreos no tripulados y para el fortalecimiento y renovación de las capacidades de vigilancia aérea del ESANT, la SEDENA invirtió la cantidad de 209,193,400 de pesos del fideicomiso público de "administración y pago de equipo militar" correspondiente al ejercicio fiscal 2016, cierto es también que con ello no lograron cumplir con el objetivo propuesto.[4]

No obstante lo anterior, se resalta que la utilización de tecnología dron, si incidió en la reducción del riesgo para el personal militar, y en gran medida ha permitido explotar la obtención de información para la generación de inteligencia en tiempo real.[5] lo que ha traído consigo importantes resultados, por mencionar la detención significativa más reciente del líder del Cartel de Santa Rosa de Lima José Antonio Yépez Ortiz alias "el marro" realizada en agosto del año 2020, gracias al empleo de aeronaves no tripuladas que operan con cámaras estadunidenses de alta resolución, con capacidad para alcanzar las 55 millas de altura, que son totalmente silenciosas y que pueden volar hasta 139 kilómetros por hora por 24 horas con-

---

4 Libro Blanco *Operación y desarrollo de la fuerza Aerea Mexicana,* SDN-LB-06, 30 de noviembre de 2012, p 37

5 Ídem p 46, 47.

tinuas.[6]

Ante lo cual resulta evidente que tanto la SEDENA como las corporaciones de seguridad estatal y municipal requiere contar con herramientas tecnológicas modernas de detección como son los sistemas aéreos no tripulados, radares, equipos de comunicación satelital, aviones, etc. que permitan lograr una ventaja estratégica en el campo de batalla que derive de una reacción y toma de decisiones oportunas.

Ahora bien, párrafos anteriores se hizo referencia a que el uso de drones debe obedecer a la preservación del orden público. El orden público implica que los derechos de los miembros de una sociedad no son absolutos, pues se hallan acotados por el respecto a las normas básicas de la organización social plasmadas en la constitución, pues de ese modo se garantiza el desarrollo armonio y general de los individuos.[7]

En ese tenor y toda vez que el uso de RPAS se ha popularizado de tal manera que su exclusividad ya no es solo militar pues en la actualidad cualquier ciudadano de forma fácil puede tener acceso a ellos, sin que exista un medio de control por parte del Estado, que permita tener plenamente la identificación de las aeronaves no tripuladas y sus pilotos cuando están siento operados.

Si bien es cierto hay una exigencia de registro a los usuarios de drones ante la Agencia Federal de Aviación Civil (AFAC) cierto es también que no se cuenta con un sistema de localización y control permanente, pues las irregularidades que pudieran llegar a presentarse con su utilización se dejan en la intención de denuncia de quienes resulten ser víctima, en el mejor de los casos cuando puedan contar con los datos de la aeronave no tripulada que causo el daño, pues de no ser así se carecería de información generando la impunidad.

---

6 "Drones, clave para capturar a 'El Marro' en su último escondite" https://www.milenio.com/policia/detencion-marro-drones-localizaron-lider-cartel-santa-rosa consultada el 7-12-20.

7 Tesis: I.3o.C.925 C , Semanario Judicial de la Federación y su Gaceta Novena Época, T. XXXIII, Abril de 2011, p. 1349

Lo que conlleva a que los usos de los RPAS queden al arbitrio de las personas incluso existiendo riesgos de vigilancias furtivas, utilización con propósitos delictivos, invasivos a la intimidad de las personas, utilización descontrolada de imágenes y datos personales. Lo anterior sin duda hace evidente la necesidad de que la legislación que regula el uso de las aeronaves no tripuladas en México, debe contemplar un control más amplio sobre su operación.

VI. NORMATIVIDAD QUE REGULA EL USO DE AERONAVES NO TRIPULADAS EN MÉXICO

En México la Secretaria de comunicaciones y transporte a través de la Agencia de Aviación Civil es la encargada de aplicar la normatividad y estándares necesarios para la utilización de los sistemas de aeronave pilotada a distancia (RPAS) en el espacio aéreo Mexicano, cuyos requerimientos yacen establecidos en la NORMA oficial mexicana NOM-107-SCT-2019 publicada en el DOF el 14 de noviembre de 2019, siendo su finalidad que la operación de los RPAS sea de forma segura, armonizada y fluida, equiparable con las operaciones de las aeronaves tripuladas.

Sin embargo dicha norma no será aplicable para operación de aeronaves no tripuladas clasificadas como autónomas, ni para los RPAS operados en espacios cerrados, en virtud de que su uso es responsabilidad del propietario de la instalación y del organizador del evento quienes deberán establecer las medidas de seguridad correspondientes, esa norma tampoco regular los drones militares, de marina y fuerza aérea, en virtud de que la operación de drones militares deberá sujetarse a las disposiciones de tránsito aéreo señaladas en el artículo 37 de la Ley de Aviación Civil, que a su vez dispone que en caso de infracciones a lo anterior se informará a las Secretarías de la Defensa y de Marina, para los efectos que procedan, pero por razones de seguridad nacional o de orden público, la Secretaría ejercerá sus atribuciones relativas a la navegación en el espacio aéreo en coordinación con las autoridades civiles o militares que correspondan.

Advirtiéndose que si bien es cierto la NOM-107 establece lo relativo a la operación de los drones en los puntos inherentes a la prevención de accidentes, protección a terceras personas, control de la conducción de aeronaves no tripuladas, peligro de la vida y de la propiedad ajena, obligatoriedad de registro de aeronaves como de los pilotos; cierto es también que no regula lo tocante a la tecnología de la cual son dotados y los alcances en su utilización, por mencionar algunos casos lo son los drones dotados de armamento letal con el que puedan privar de la vida a una persona.

Es decir, la laguna que en su regulación se presenta incide en la falta de control tanto del equipamiento del que puedan ser dotados de manera furtiva los drones, como de su operación en tiempo real, en virtud de que no existe un sistema de geolocalización a través del cual las autoridades encargadas de reglamentar su uso puedan saber los lugares en que se desplazan.

VII. REGLAMENTACIÓN INTERNACIONAL COMO REFERENTE EN EL USO DE TECNOLOGÍA DRON

A nivel internacional los RAPAS son regulados por la Organización de Aviación Civil Internacional (OACI) cuyas disposiciones tienen carácter orientador tendiente a lograr que el tráfico aéreo sea seguro a través de metodologías y protocolos unificados entre las naciones, es decir, aun y cuando cada país miembro tiene la libertad de determinar la normatividad aplicable, deben ceñirse a los parámetros que plantea la organización, varios países de Latinoamérica forman parte de ella, incluido México.

Las aeronaves no tripuladas han sido blancos de múltiples opiniones tanto a favor como en contra, no obstante, su uso sigue incrementándose, la inversión mundial en el sector de los RPAS alcanzara los 114,000 millones de dólares para el 2023, encabezando la lista EUA[8] país en donde los RPAS han sido utilizados con más auge en las actividades de política militar exterior.

8 Muñoz Villareal, Alberto, Coord. *Inteligencia artificial y riesgos cibernéticos responsabilidades y aseguramientos,* Valencia, ed. Tirant to Blanch, 2019, p. 172

En consecuencia, el argumento respecto a la dicotomía de las ventajas y desventajas que conlleva el empleo de los RPA en actividades militares en los Estados Unidos, obedece a la secrecía en sus operaciones, lo que permite que la información que se hace pública sea sesgada, limitada y controlada por quienes tienen el control de los medios de comunicación o por grupos cuyos intereses son contrarios a las políticas del Estado o afines al mismo, información que indudablemente influye en la condena que los ciudadanos hacen del uso de los RPAS.

Sumado a que en Estados Unidos los RPA son empleados como armamento, y sus misiones en muchas ocasiones son "asesinatos selectivos", es decir asesinatos cometidos bajo el amparo del silencio y la invisibilidad; se trae a colación el asesinato a control remoto o a la distancia, recientemente perpetrado en la administración de Donald Trump en contra del General Irani Qasem Soleimani a principios del año 2020, hecho que permite evidenciar la notabilidad de la tecnología de aeronaves conducidas a la distancia a control remoto.

Sin dejar a un lado que no solo son cometidos asesinatos hacia un blanco establecido pues según cifras ofrecidas por *the boreau of investigativa journalism* de enero de 2015 a enero de 2019 entre 700 y 1700 civiles han muerto producto de los ataques con drones de los cuales casi 400 serían niños.[9]

Lo alarmante de ello es que, como en el caso de las armas nucleares, Estados Unidos fue de los pioneros en obtener esta clase de capacidad, en palabras del Dr. Micah Zenko, un miembro del Consejo de Relaciones Exteriores "durante la próxima década, el casi monopolio estadounidense en ataques con drones se deteriorará a medida que más países desarrollen y perfeccionen esta capacidad"[10],

9 https://www.laestrella.com.pa/internacional/america/200201/200131-politica-asesinatos-selectivos-eeuu consultado el 25-11-2020

10 https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-27_Issue-1/2015_1_05_chapa_s.pdf consultado el 25-11-2020

lo que sin duda invita a la reflexión de que Estados Unidos así como pudo moldear el uso de las armas nucleares muy probablemente lo puede hacer con el de drones, la diferencia es que a nivel internacional la consciencia del daño que produciría el uso indiscriminado del armamento nuclear permea en todas las naciones, lo que no ocurre con el uso de los drones ante lo reciente de su tecnología.

Por otro lado, en la Unión Europea, el comité económico social europeo en su dictamen sobre una nueva era de la aviación, regula los aspectos de la privacidad y colaboración institucional en este sector innovador, el reglamento de la unión europea 2116/679 del parlamento Europeo y del consejo de 27 de abril de 2016 antepone en el uso de drones, las razones de seguridad publica así como la protección a las personas físicas en lo relativo a datos personales y libre circulación de estos, ante el contexto actual en el que "los datos son la moneda de la economía digital de hoy"[11] dando especial importancia al rubro del derecho a la privacidad.

Su normatividad atiende también a las circunstancias de operaciones de drones civiles, ya que en el mismo espacio aéreo confluyen aeronaves tripuladas como las que no lo son; establece igualmente obligatoriedad para que las personas que participan en la operación de una aeronave no tripulada, incluido el piloto a distancia deben disponer de los conocimientos y las destrezas necesarios para garantizar la seguridad de la operación, así mismo, abordan el tema de los requisitos medioambientales, estableciendo un umbral mínimo para el registro de los operadores de aeronaves, que deberán registrarse si operan con drones que puedan transmitir más de 80 julios[12] de energía cinética en caso de colisión.

Siendo importante resaltar que la unión Europea se ha preocu-

---

11 Muñoz Villareal, Alberto, Coord. *Inteligencia artificial y riesgos cibernéticos responsabilidades y aseguramientos,* Valencia, ed. Tirant to Blanch, 2019, p. 175

12 Del ingl. *joule,* y este de J. P. *Joule,* 1818-1889, físico inglés. m. Fís. Unidad de trabajo del sistema internacional, que equivale al trabajo producido por una fuerza de1 *newton* cuyo punto de aplicación se desplaza 1 metro en la dirección de la fuerza. (Símb. J). https://dle.rae.es/julio

pado por implementar medidas para informar a su sociedad respecto a los ordenamientos legales aplicables en el uso de drones, entre las estrategias empleadas es la creación del sitio web *dronerules.eu*, pagina pública y de fácil acceso para consultar la normatividad que rige en cada lugar de la unión Europea, acerca del uso de drones.

Ahora en particular, por lo que respecta a España el uso civil de drones está sujeto a la legislación aeronáutica civil, en la que se establecen límites y obligaciones para su uso, limitándolo a la realización de trabajos aéreos con actividades de investigación; observación y vigilancia de incendios forestales, publicidad aérea u operaciones de emergencia, búsqueda y salvamento, llevan un control estricto ante la obligatoriedad legal de que todos los RPA deben portar una placa con todos los datos de la nave, del fabricante y del piloto.

La agencia Española de seguridad aérea exige un certificado de aeronavegabilidad para operar un RPAS que tenga una masa superior a 25 kg, incluso establece reglas específicas para el uso recreativo de los drones[13], regula lo relativo a la responsabilidad por daños causados por las compañías aéreas, sin embargo el real decreto no es aplicable a los RPAS militares ni a los que tienen un peso superior a 150 kg,

En Canadá el uso de los drones, tiende a la aplicación de las regulaciones de tránsito, lo que sin duda incide en la reducción de accidentes vehiculares y faltas al reglamento, pues los ciudadanos se saben vigilados permanentemente de modo que se ven obligados a cumplir los ordenamientos legales, de igual forma han logrado la captura de sospechosos durante la noche gracias a las cámaras térmicas con que equipan a los drones.[14]

---

13 Muñoz Villareal, Alberto, Coord. *Inteligencia artificial y riesgos cibernéticos responsabilidades y aseguramientos,* Valencia, ed. Tirant to Blanch, 2019, p. 189

14 *Análisis jurídico del uso de Drones,* http://ri.uaemex.mx/bitstream/handle/20.500.11799/99170/Trabajo%20Terminal%20de%20Grado%20OSCAR%20FERNANDO%20CASTA%C3%91EDA%20BASTIDA%20%281%29.pdf?sequence=1&isAllowed=y p. 45 consultado el 2-12-2020.

Ante todos los usos que a nivel internacional se da a los RPAS, se destaca la especial atención que las legislaciones ponen a la capacitación que deben tener los usuarios de tecnología dron, el registro y control de los mismos, ante el riesgo que conlleva la utilización sin práctica ni conocimientos, que sin duda puede poner en peligro a la comunidad, su patrimonio social, cultural y económico.

Cierto es que, bajo una detallada planeación el uso de drones puede aportar grandes ventajas en reducción de personal y tiempo en actividades en donde la presencia del hombre no es indispensable, incluso en tareas sucias, aburridas o peligrosas para los humanos. Lo importante será visualizar la operatividad de los drones no para desplazar a los humanos en ciertas tareas sino para aportar beneficios a las mismas.

VIII. CONCLUSIONES

La política criminal en su definición restringida tiene en uno de sus diversos tópicos, la actualización de los cuerpos represores del Estado. Su justificación, la aplicación estricta y regulada del poder para combatir y prevenir los delitos o la seguridad nacional. La ciencia y la tecnología, van de la mano con el derecho penal para hacerlo más científico y útil a la sociedad y el sistema de poder.

Los drones son un avance tecnológico hoy vital para cumplir la tarea de control social inscrita en la seguridad que brinda el Estado. Su uso deberá facilitar la vigilancia y la recolección de información para anticipar los peligros que representan los terroristas y abusivos. Ver a los lejos será un arma sorpresa que requerirá de regulación constante que marque los límites del Estado entre los espacios público-privado.

Sin duda, los drones también usados por los criminales para cumplir sus fines por lo cual, la limitación, registro y control de los mismos es una tarea urgente, de lo contrario se podría perder dominio público al usar el espacio aéreo con fines perversos.

Pero no todo en las políticas de uso de armas y drones es positivo, toda política criminal encierra la tentación de usar el poder del Estado con fines autoritarios. Los drones, también son una herramienta de espionaje de adversarios o de sujetos considerados peligrosos para el Estado. Vigilar lugares y personas es una tarea común y peligrosa ante el discurso formal garantista. Los drones pueden entrar a espacios tan íntimos que la información recogida en tiempo real puede ser usada desde otras tecnologías dejando al individuo expuesto a la represión estatal y a la extorsión.

Los drones son vigilancia y arma desde los cielos donde los límites del ojo humano se ve imposibilitado. Ver e informar puede ser una noble tarea preventiva siempre y cuando no caiga en los usos facciosos. La policía civil tiene el deber de actualizarse y tecnificarse para cumplir la función pública de la seguridad, vigilemos entonces los discursos que veladamente dictan controles parciales y minimizan el desarrollo vertiginoso de esta tecnología. Vengan pues políticas criminales donde la tecnificación sea por el ciudadano y no una retórica más donde "vigilarnos no sea nada nuevo".

IX. FUENTES DE CONSULTA
Bibliografía

Bauman, Zygmunt. Miedo Líquido, La sociedad Contemporánea y sus temores. México, Paidós, 2013.

Bauman, Zygmunt, Comunidad. En busca de la seguridad en un mundo hostil. Madrid, 2003

Bauman, Zygmunt y Lyon, David. Vigilancia Líquida. Barcelona, 2017

López Velarde, Samuel Chacón, *Los Drones y su Legislación en México,* Ciudad de México, Tirant lo Blanch, 2017.

Luhmann, Niklas. México, Poder ,Anthropos-Universidad Iberoamericana.2005.

Muñoz Villareal, Alberto, Coord. *Inteligencia artificial y riesgos cibernéticos responsabilidades y aseguramientos,* Valencia, ed. Tirant to Blanch, 2019.

Navarro, Bonilla, Diego y otros. Terrorismo Global. Gestión de Información y servicios de inteligencia, Madrid, Plaza y Valdes, 2007

Servera, Muntaner, José Luis. Ética Policial, Valencia, Tirant lo Blanch, 2000

Orwell, George, 1984, México Destinolibro, 2000.

Hemerografía

Alvarez, León, José Antonio. *"Construcción de la imagen de la seguridad o control social multidimensional"* Rev. Posgrado en Derecho,Vol 3, núm 5, Julio diciembre 2007, México, UNAM. P 97

Cibergrafia

Real Diccionario. Real Academia Española. Consulado en: https://dle.rae.es/espiar consultado. Enero 21/21.

Reyes, Eréndira. "Los Drones se Vuelven Aliados de la Ciberdelincuencia". Fuente electrónica, tomado de: https://expansion.mx/tecnologia/2019/09/03/los-drones-se-vuelven-aliados-de-la-ciberdelincuencia Febrero 9, 21

http://etimologias.dechile.net/?dron#:~:text=La%20palabra%20dron%20(avi%C3%B3n%20o,no%20tripuladas%2C%20por%20su%20zumbido (18 nov 2020)

https://www.appliedaeronautics.com/albatross-uav (18 nov 2020)

https://www.milenio.com/policia/detencion-marro-drones-localizaron-lider-cartel-santa-rosa "Drones, clave para capturar a 'El Marro' en su último escondite" (7 dic 2020)

https://www.laestrella.com.pa/internacional/america/200201/200131-politica-asesinatos-selectivos-eeuu (25 nov 2020)

https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-27_Issue-1/2015_1_05_chapa_s.pdf (25 nov 2020)

http://ri.uaemex.mx/bitstream/handle/20.500.11799/99170/Trabajo%20Terminal%20de%20Grado%20OSCAR%20FERNANDO%20CASTA%C3%91EDA%20BASTIDA%20%281%29.pdf?sequence=1&isAllowed=y p. 45 "*Análisis jurídico del uso de Drones*" (2 dic 2020)

https://dle.rae.es/julio (25 dic 2020)

Otros Documentos.

Libro Blanco *Operación y desarrollo de la fuerza Aérea Mexicana,* SDN-LB-06, 30 de noviembre de 2012, p 37

Jurisprudencia.

Tesis: I.3o.C.925 C , Semanario Judicial de la Federación y su Gaceta Novena Época, T. XXXIII, Abril de 2011, p. 1349

EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN EN LA POLÍTICA CRIMINAL: CONTROL Y VIGILANCIA

Jorge Ignacio Jiménez Martínez*
Roberto Álvarez Manzo**

SUMARIO: I. Introducción. II. La Virtualidad. Tecnologías de la Información y Comunicación. II. El Control y Vigilancia por vía de las TIC'S. III.Obstaculización del Control y Vigilancia por las TIC's. IV. Epílogo. Funcionalidad de las Tecnologías de la Información en la Política Criminal.

I. INTRODUCCIÓN

La virtualidad como un entorno de la realidad, es construida por la integración de las relaciones entre máquina humano, bajo un lenguaje universal de códigos específicos, que permite la comunicación y la interacción tanto de sujetos como de máquinas o Tecnologías de la Información y Comunicación en una red datos. El flujo constante, atemporal y global de la información, permite por un lado la detección e identificación de los sujetos, bajo procesos de control y vigilancia; por otro lado, procesos de resistencia, de anonimato u ocultamiento, de los sujetos, que ingresan al ambiente virtual.

El apoderamiento de la virtualidad, para el control y la vigilancia de los individuos, es potencializado por el proceso de modernización que se caracterizan por la ruptura conceptual del espacio y el tiempo, permitiendo extraer de las personas

los datos necesarios para su identificación; todo esto, con el objetivo de generar las pautas de verdad y de poder necesarias, en la justificación y regulación de las relaciones o interacciones de dominio de la información en los entornos virtuales.

---

* Jorge Ignacio Jiménez Martínez es Licenciado en Derecho y Maestro en Política Criminal por la Facultad de Estudios Superiores Acatlán.
**Roberto Álvarez Manzo es Licenciado en Sociología, Maestro en Política Criminal y Profesor por la Facultad de Estudios Superiores Acatlán.

II. LA VIRTUALIDAD. TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Los individuos son Seres construidos de información perceptible, que se expresa en signos significantes; dentro de símbolos nos contemplamos y observamos el entorno de la realidad. Tal afirmación, no pretende alejar el entendimiento del Ser biológico-físico: Todo lo que Es y Está, pertenece a una dinámica dentro de un espacio y tiempo particular, que se manifiesta y percibe por símbolos; la existencia, el movimiento y el espacio-tiempo, solo son posibles en la medida de la información que se aprehende, procesa y expresa por vía de la inteligencia de los Seres.

Por inteligencia se entiende al potencial biológico y psicológico de los Seres, que permite el manejo y procesamiento de la información, para la planificación, la solución de problemas, la toma de decisiones, el pensamiento abstracto y la generación de productos dentro de la sociedad[1]. El proceso mental de la inteligencia, como capacidad y potencial, permite la configuración de la existencia, la dinámica y el espacio-tiempo, que se aprehenden y manifiestan por la información, por los símbolos significantes, que además permite la interacción de los sujetos, dentro de un colectivo particular.

La información[2] manipulada y gestionada por la inteligencia, construye y fija en estructuras subjetivas de pensamiento a la realidad: Somos producto de la mente, de esa naturaleza; todo pasa por su creación, por su fuerza constructiva y destructiva, el ser, su movimiento, el espacio y tiempo de ocupación solo es posible en

---

1 *Cfr.* Villamizar, Gustavo y Donoso, Roberto, *Definiciones sobre inteligencia. Revisión histórica,* en: Psicogente, 16 (30), pp. 407-423. Julio-Diciembre, Universidad Simón Bolívar. Barranquilla, Colombia, 2013.

2 "La información es un conjunto organizado de datos que constituyen un mensaje sobre un determinado ente o fenómeno". Torres Garibay, Rodrigo, *Tecnologías de Información y comunicación en las Organizaciones,* en: Reyes Echeagaray, Dora Alicia (Coord.) *Tecnologías de Información y comunicación en las Organizaciones,* Facultad de Contaduría y Administración, Publicaciones Empresariales UNAM. FCA Publishing, Ciudad Universitaria, México, 2015, p. 13.

un proceso de inteligencia que construye una realidad subjetiva y particular para cada individuo, que se proyecta o expone dentro de diversos entornos de interacción por vía de los procesos de comunicación.

La comunicación como proceso de transferencia de información, de símbolos significantes entre uno o múltiples emisores y receptores, por vía de un código reconocido y un medio o canal determinado[3], permite que la realidad se exponga, como una cualidad de los objetos, de los fenómenos, de todo aquello que entra en dinámica, dentro de un espacio y tiempo particular; cualidad que por medio de la inteligencia se verifica y otorga el conocimiento necesario, para generar la certidumbre en los sujetos de que lo perceptible es real con características determinadas, conforme a los símbolos significantes que permiten la interacción en los entornos[4].

El contexto principal de la realidad se comprueba en la vida cotidiana de los individuos, es decir en la vida en sociedad, que se presenta ante ellos como una serie de elementos causales, significativos e intersubjetivos ordenandos e interpretados de forma coherente, que son otorgados con la característica de realidad, por el acuerdo entre individuos y por las estructuras de pensamiento subjetivo, así como por las acciones e interacciones que se despliegan por tales estructuras.[5]

Retomando las ideas expuestas para su clarificación, la realidad como proceso se fija en la mente de los sujetos y desde ella es proyectada en entornos de interacción por vía del proceso de comunicación; tales entornos son delimitados por símbolos significantes compartidos por otros individuos de manera intersubjetiva; la realidad, su proyección permite la relación de sujetos, personas o entidades sean mate-

---

3 *Cfr.* Torres Garibay, Rodrigo, *Tecnologías de Información y comunicación en las Organizaciones,* Op. Cit., p. 14.

4 *Cfr.* Berger, Peter L., Luckman, Thomas, *La construcción social de la realidad,* Amorortu Editores, Buenos Aires, Argentina, 1999, p. 13.

5 *Ibidem.,* p.37.

riales o inmateriales, estructurándose como una construcción social de comunicación de la información que se perfecciona para su comprobación, por las múltiples y exponenciales acciones y combinaciones de pensamiento de los miembros inmersos en la colectividad.

La transferencia de información, por vía de los procesos de comunicación, permiten no solo la generación de un entorno material de la realidad, sino de entornos ideales o virtuales; es decir, la interacción de los sujetos por símbolos significantes, permite la producción de realidades teóricas, dentro del campo de las ciencias fácticas o formales; o bien la generación de entornos virtuales de la realidad donde el conocimiento y el procesamiento o manipulación de la información se realiza no de forma exclusiva por los sujetos, sino en grado equiparable con una inteligencia artificial, que permite una interacción compleja entre individuo y máquina, ambos en un plano de similitud.

En consonancia, la virtualidad se manifiesta por la integración de la inteligencia artificial y humana para la creación de ambientes que extractan fenómenos u objetos de la realidad, con la finalidad de ser operados o manipulados de manera sintética, mediante la conexión del sujeto físico al mundo virtual, por medio de las tecnologías de la información y la comunicación. La emulación de la realidad en un entorno virtual requiere de forma esencial la transferencia de información, a través de un código, entendible tanto para el usuario físico, como para la máquina, que permita la inmersión del sujeto en el entorno virtual, bajo un lenguaje y lógica coincidentes.[6]

Resalta así que, la virtualidad de la realidad como entorno, se proyecta sobre aspectos digitales, electrónicos, mecanismos de inteligencia artificial, codificada y decodificada por instrumentos téc-

---

6 *Cfr.* Heras Lara, Lizbeth y Villarreal Benítez José Luis, *La realidad virtual en los nuevos paradigmas de la ciencia de datos*, Revista Digital Universitaria, 1 de septiembre 2011, Volumen 12, Número 9, Coordinación de Acervos Digitales, Dirección General de Cómputo y de Tecnologías de Información y comunicación, UNAM, pp. 3 y 4, en: http://www.revista.unam.mx/vol.12/num9/art87/art87.pdf consultado: mayo 2019.

nicos, en suma, herramientas, tangibles e intangibles de estructuras lógicas, necesarias para acceder y manifestar la realidad de los sujetos en dicho ambiente virtual. Las tecnologías de la información y comunicación (TIC´s)[7], se visibilizan de esta manera, como los medios y herramientas por donde la codificación de la información de la realidad ingresa al medio para su decodificación por la inteligencia artificial, y su manifestación que interactuará con los demás individuos que ingresan al entorno.

La información no solo es vital para la configuración de la realidad por símbolos significantes, sino también para la manifestación o proyección de esta a partir de la inteligencia de los sujetos y la generación de relaciones entre individuos; en caso concreto, el medio digital se soporta de manera esencial en la información, su transmisión, manipulación, procesamiento y acumulación, en un constante archivo de datos, sobre un sistema reticular que permite múltiples conexiones de forma interactiva entre sujetos-máquinas-sujetos.[8]

El entorno virtual de la realidad, requiere del flujo constante de información misma que es almacenada dentro de una memoria histórica y artificial bajo un tiempo flexible, para ser extendida sin limitación de espacio, por medio de las TICS, que codifican y recodifican la información para su exposición en un solo tiempo y en todo el cumulo de sujetos que interactúan dentro del medio. Con lo antes dicho, se identifica la necesidad de los medios digitales, TIC'S, para el acceso de los sujetos a la información, a la manipulación y su expresión dentro de la realidad virtual, así como para la

---

7 "Podemos describir en términos generales a las Tecnologías de la Información y Comunicación como un conjunto de elementos compuestos por herramientas, prácticas y técnicas que son utilizados para el tratamiento, procesamiento, almacenamiento y transmisión de datos con la finalidad de estructurarlos en información útil que derive en la solución de problemas y la generación de conocimiento". Torres Garibay, Rodrigo, *Tecnologías de Información y comunicación en las Organizaciones*, Óp. Cit., p. 14.

8 *Cfr.* Bravo Ramírez, Leticia, *et al*, *Análisis de las tecnologías de la información y de la comunicación (TIC'S) en México*, p. 2, obtenido en: www.paginaspersonales.unam.mx consultado: 5 de junio de 2019.

generación de interacciones dentro del ambiente, que no es limitado por un espacio físico o un tiempo particular.

De tal suerte que, la realidad virtual es determinada en su amplitud y capacidad, conforme al flujo, manipulación y almacenamiento de la información digital, que es generada por vía de las TIC'S en conexión con los sujetos usuarios del entorno. Así se permite expresar que las herramientas digitales de información y comunicación a más del soporte físico (*Hardware*) y lógico (*Software*), se complementan con el componente humano, en un proceso de adaptación y capacitación dentro de un ambiente digital, donde usuario y máquina (Inteligencia Humana e Inteligencia Artificial) se transforman recíprocamente, con la finalidad de atender necesidades propias del entorno virtual y de las interacciones que en este se proyectan y generan.[9]

En consecuencia, el entorno digital es medido por la cantidad de interacciones: usuario-máquina, que se ejecutan expresamente, o bien que tienen el potencial de ejecutarse, donde cada dispositivo o tecnología para transferir y recibir información, vinculada a un sujeto usuario, marca la dimensión real del entorno; entonces, cada dispositivo digital permite en potencia el flujo de información, aun cuando este se encuentre suspendido, pero que, en sí, marca la dimensión de la virtualidad.

Ahora bien, la funcionalidad de las TIC´s, sea de manera pasiva o activa en el entorno, vistas como nodos de información en una red, capturan, archivan y difunden la información que es almacenada, para su posterior utilización e interacción, permitiendo así la generación de una o múltiples copias de información, que son accedidas y archivadas en los medios digitales, difundidas y dirigidas

---

9 *Cfr.* Fabres Barahona, Juan Carlos *et al.*, *Análisis del uso de las Tecnologías de la Información y la Comunicación en los establecimientos educacionales de Chile: Caso del Colegio Santo Tomás de la Comuna de Ñuñoa,* Seminario para optar al Título Profesional de Ingeniero Comercial mención Administrativa, Universidad de Chile, Santiago de Chile, 2014, p. 10 y 11, obtenido en: http://repositorio.uchile.cl/handle/2250/116586 consultado: 6 de junio de 2019.

desde ahí, para su visualización y nueva difusión. Las copias digitales de información son los entes binarios que permiten la existencia, de un "yo-virtual", que se relaciona y actúa dentro del entorno, por la información que se transmite y recibe de forma activa o pasiva.

Por otra parte, las interacciones de los sujetos en la realidad, desde la intersubjetividad de los significantes, permiten la creación de pautas o reglas, con la finalidad de estructurar esquemas de pensamiento tendientes a normalizar, vigilar y controlar a los individuos, bajo códigos de relación y comunicación, asumidos y comprendidos de forma mayoritaria por los individuos que se relacionan en los ambientes; dichos esquemas de pensamiento delimitan, califican y clasifican los medios y mecanismos, por los que se proyectan y asimilan los objetos o fenómenos inmersos en el entorno de la realidad. En el caso que nos ocupa, la inteligencia artificial, los medios digitales de transferencia de información, así como las leyes lógicas y materiales fijadas en la inteligencia de los sujetos, marcaran las pautas, reglas o protocolos a seguir, para la interacción de los individuos en la virtualidad.

Operando por medio de las Tecnologías de la Información y Comunicación, la virtualidad de la realidad requiere de pautas, protocolos o reglas, dentro del medio digital, y fuera del mismo, en los ambientes materiales e ideales de la realidad; una existencia física de un sujeto puede generar múltiples existencias de información; una multiplicidad de información consigue generar procesos o estructuras de pensamiento, diversas a los controles lógicos de las ideas. Las TIC´s y la virtualidad se presentan así, como una herramienta polimórfica para los fines e intereses de los sujetos que las emplean; resaltando los de control y vigilancia sobre los sujetos, su actividad, relaciones y dinámicas, la información en sí que representa la virtualidad, por parte de organizaciones de gobierno o particulares, que se aventajan de los medios digitales para la culminación de sus objetivos.

II. EL CONTROL Y VIGILANCIA POR VÍA DE LAS TIC´S.

La presencia de modalidades disposiciones y operaciones dirigidas al control de las personas, vía identificación y vigilancia, cuentan con una historia extensa y compleja en occidente. Por ejemplo, para el caso europeo Ilsen About y Vincent Denis exponen en su texto Historia de la identificación de las personas este devenir en el último milenio. La obra analiza el tema dividiéndolo en 5 etapas que comprenden: 1) la identificación en la época medieval entre los siglos XVI al XV, 2) la identificación asumida por el Estado y por lo escrito en los siglos XV al XVIII, 3) la identificación en la época del Estado-nación en el siglo XIX, 4) el camino hacia la identificación de masas a finales del siglo XIX hasta la segunda guerra mundial y, finalmente, 5) los regímenes de vigilancia en el contexto de las tecnologías informáticas de mediados del siglo XX a principios del XXI.

En líneas generales, las características de las etapas ante dichas se definen de la siguiente manera: La primera se distingue "por el importante lugar del cara a cara, la instrumentación de múltiples señas de identidad, los inicios de la identificación a distancia bajo la tutela de las formas de autoridad pública que se imponen entonces." Para la segunda etapa los autores establecen que "el papel de la identificación escrita se refuerza considerablemente, mientras se multiplican registros y documentos de identidad, que coexisten con maneras de identificar ligadas al cara a cara y al conocimiento mutuo." En la tercera fase pueden advertirse una serie de inflexiones con motivo de la aparición de una nueva estructura política en el continente europeo. Los autores señalan al respecto el advenimiento de "el estado-nación, que tiene por consecuencia la estatalización y la nacionalización de la identificación." La cuarta etapa aparece "después de la primera Guerra Mundial, [dónde] los estados europeos dan una importancia fundamental a la atribución a todos los individuos de una identidad cierta; [considerando que] los regímenes totalitarios se caracterizan también por una definición exclusiva

de las identidades y las medidas coercitivas de identificación." Por último, los autores afirman la presencia de Procedimientos dirigidos a la identificación de masas, donde los medios tecnológicos soportan este ejercicio en el contexto "de un nuevo umbral representado por la informatización de los datos y la difusión de las técnicas de vigilancia" hasta hoy.

A través de obras como la citada es posible atestiguar la presencia, para el caso europeo (con las obvias influencias que estos ingenios tienen en las naciones periféricas), de una lógica centrada en la identificación de las personas, misma que como puede observarse, ha tenido un desenvolvimiento caracterizado por lo complejo, pues han sido diversas las modalidades y utilidades que esta dinámica presenta en su temporalidad. En ocasiones, se atestigua la manera en la cual los procedimientos identificatorios guardan relación con auto-afirmaciones identitarias, como es el caso de la heráldica y el despliegue de signos de poder presentes en la primera etapa. Por otra parte, puede observarse cómo la presencia y desenvolvimiento de la identificación de las personas presenta giros en función de cambios políticos, económicos, sociales y culturales, al grado de convertirse, paulatinamente, en un procedimiento de control social apetecible para la gestión de la dominación por parte de las estructuras y sectores dominantes dentro de una colectividad, tal como paulatinamente fue ocurriendo.

Para efectos del presente escrito, dirigimos nuestra atención en la última de las etapas referidas, sin menoscabo de la presencia, condiciones, características, así como las posibles influencias, que las anteriores fases tengan con el contexto actual, en función de la pretensión general de nuestro trabajo, la cual gira alrededor del análisis del impacto que las actuales tecnologías informacionales y comunicativas tienen respecto del control social y la política criminal, vía los procedimientos puestos en juego por los dispositivos encaminados a las labores de inteligencia, presentes tanto en el sector público como el privado.

Considerando la actual presencia de tecnologías que potencian las labores de vigilancia, control y detección de las personas, cabe destacar que existen posicionamientos diversos. Por ejemplo, se puede enunciar lo planteado por Zygmunt Bauman, quien en su obra *La sociedad sitiada*[10] aborda el complejo relacionado con la presencia de la televisión y sus implicaciones en materia de construcción de la realidad. En el capítulo de dicha obra que por nombre lleva "Como se ve en tv" el autor aborda la polémica aprobatoria y reprobatoria relacionada con las tecnologías, a partir de los ejemplos del panglosianismo y el casandranismo. Para el caso del primero se refiere a los planteamientos que desmedidamente caen en un triunfalismo apologético de las tecnologías. La refutación a lo antedicho tendrá su base en las consideraciones fundamentadas a partir del mito casandriano que Zygmunt Bauman plantea como parte de las posturas que férreamente se oponen a la presencia de la tecnología por considerarla un ingenio dirigido a pervertir el ideario humano. Considerando dichas posturas es posible atestiguar la naturaleza del debate entre luditas y golemistas, misma que posiciona a la tecnología en medio de la controversia entre sus posibles efectos positivos y emancipatorios, contra los testimonios que dan fe de los efectos perniciosos y alienantes para la vida de las personas.

De manera semejante, y como complemento en alcance de lo referido, Umberto Eco formula una mención que se antoja similar a la planteada por Zygmunt Bauman, al hablar en su texto *Apocalípticos e integrados*[11] respecto a posicionamientos diversos relacionados, en este caso, con la comunicación masiva, misma que por la lógica de su condición mediática juega la suerte de la tecnología en lo general. Para el caso de los integrados, el autor fija su posición vinculada a la aprobación desmedida e irreflexiva de los beneficios que la comunicación masiva, mediada por la tecnología, presenta,

---

10 *Cfr.* Bauman, Zygmunt. *La sociedad sitiada*, Fondo de Cultura Económica, México, 2011.

11 *Cfr.* Eco, Humberto, *Apocalípticos e integrados,* Editorial Lumen, España, 1984.

mientras que para el caso de los apocalípticos, la denominación refiere el posicionamiento de aquellos sectores críticos a ultranza que observan las peores perversiones a la condición humana promovidas por la presencia de los medios masivos de comunicación y las tecnologías que los hacen posibles, algo similar a lo que Theodore Kaczynski entendía por el atrofiamiento de la capacidad de poder, en desmedro de la condición humana.

La presencia de tecnologías informacionales y comunicativas centradas en operativizar y potenciar la vigilancia, el control y la detección de las personas, puede ser interpretada desde diferentes ópticas, como ya se ha dicho respecto al debate existente sobre la tecnología en lo general. Nosotros hemos decidido explorar la vertiente centrada en el encaminamiento de las tecnologías hacia procedimientos de control social, en función de una razón que nos parece lógica, la cual, surge por la inquietud derivada de los planteamientos que afirman y soportan, con bases y fundamentos, la existencia de procedimientos dirigidos al control alienante de los seres humanos, implementado a partir de estos ingenios tecnológicos. Si las afirmaciones críticas respecto a la utilización de la tecnología para finalidades draconianas es cierta, ello nos coloca ante la imperiosa necesidad de examinar, detalladamente, la presencia de dichos ingeniosos, por cuánto a las posibles problemáticas que de ellas surgen, (mismas que, conforme a las posturas críticas que las han denunciado) se deduce en su presencia y operatividad como auténticos riesgos para el desarrollo de una condición de vida humana, donde pueda garantizarse un mínimo de circunstancias afables para la coexistencia pacífica y equitativa.

Una primera consideración al respecto la identificamos por cuanto a que las nuevas tecnologías informáticas y comunicativas, potenciadas con el proceso modernizador,[12] han mostrado una faz perniciosa, al ser utilizadas para finalidades mezquinas en activida-

12 *Cfr*. Beck, Urlich. *La sociedad del riesgo mundial. En busca de la seguridad perdida*. Barcelona. Paidíos. 2008. Urlich Beck es un autor paradigmático por cuanto a la crítica

des de vigilancia, detección y extracción de información de las personas. Una afirmación, que de manera genérica encuadra estas críticas, es la planteada por Gilles Deleuze en el retrato que nos ofrece sobre las sociedades de control. El autor ejemplifica estos hechos al señalar en analogía que: "Los anillos de una serpiente son aún más complicados que los agujeros de una topera."[13] El autor plantea así, en su escrito *Posdata sobre las sociedades de control*, el apotegma distintivo de una era caracterizada por la presencia de formas de control social inéditas por cuanto a sus antecesoras. Retrospectivamente Gilles Deleuze distingue, para occidente, dos épocas anteriores a las sociedades de control, caracterizadas por la soberanía y la disciplina. Las primeras se distinguían de las segundas por aspectos específicos tales como: "recaudar más que organizar la producción, decidir la muerte más que administrar la vida."[14] Constituyen sociedades enfocadas en el posicionamiento potenciado de la figura soberana respecto de aquellas circunstancias y condiciones sobre las cuales su poder puede recaer. Cosa diferente es el advenimiento, entre los siglos XVIII y XIX, de las sociedades disciplinarias, las cuales, en la óptica del propio Gilles Deleuze quien da continuidad a las ideas propuestas por Michel Foucault, plantea se distinguen por un control claustral férreo de los individuos. La sujeción de la que son objeto los seres humanos los determina a una lógica alienante de control en el cual, docilidad y utilidad, serán los frutos deseados producto de ese encierro condicionante a una dinámica de sometimiento, dirigida a producir en el sujeto la mayor potenciación de sus fuerzas explotables. En contraposición con lo anterior, Gilles Deleuze desarrolla los planteamientos explicativos que dan cuenta de las sociedades de control, mismas que se caracterizan por

---

respecto a la tecnología y sus posibles riesgos para la vida social.

13 Deleuze, Gilles, *Posdata sobre las sociedades de control*, obtenido en: https://www.fundacion.uocra.org/documentos/recursos/articulos/Posdata-sobre-las-sociedades-de-control.pdf p. 4, consultado: 12 de noviembre de 2019.

14 *Ibidem.*, p. 1.

la flexibilidad, apertura o adaptabilidad de las formas de dominación que pesan sobre los otrora individuos, mejor denominados en este contexto como dividuos. Sobre ello el propio autor señala:

> No es necesaria la ciencia ficción para concebir un mecanismo de control que señale a cada instante la posición de un elemento en un lugar abierto, animal en una reserva, hombre en una empresa (collar electrónico). Félix Guattari imaginaba una ciudad en la que cada uno podía salir de su departamento, su calle, su barrio, gracias a su tarjeta electrónica (dividual) que abría tal o cual barrera; pero también la tarjeta podía no ser aceptada tal día, o entre determinadas horas: lo que importa no es la barrera, sino el ordenador que señala la posición de cada uno, lícita o ilícita, y opera una modulación universal.[15]

El tema propuesto nos introduce tanto a una época como una lógica caracterizadas por la implementación de modalidades operativas y estructurales, destinadas al control social de los individuos y la población, llevadas a cabo por su naturaleza dúctil, maleable, abierta y adaptable a prácticamente cualquier circunstancia, sin necesidad de comprometer condiciones, contexto o entramado, a modalidades de encierro o condicionamiento a ciertos espacios con limitaciones y barreras específicas. En este sentido, las sociedades de control se muestran a la manera de conglomerados dispuestos de forma tal que hacen posible el alcance de los instrumentos y mecanismos de dominación social a prácticamente cualquier sitio, introduciendo una lógica de deslocalización extendida a cualquier rincón donde la vigilancia y la detección de los seres humanos se juega de forma mucho más accesible, continua y cuasi automática.

Si bien la tecnología no es el único elemento al cual podemos atribuir la causal fundamental para el surgimiento de este tipo de sociedades, si cabe mencionar que resulta una pieza fundamental en la constitución de este nuevo rompecabezas. La presencia de las

15 *Ibidem.*, p. 4.

tecnologías informacionales y comunicativas se hace patente en el propio escrito de Gilles Deleuze, pues para mencionar un caso, cita la existencia del brazalete electrónico, como elemento distintivo de esta sociedad que no requieren de espacios carcelarios disciplinarios cerrados para mantener el control por cuanto a la ubicación, vigilancia y detección, de aquellas personas sujetas a su acción. El brazalete electrónico posibilita el intercambio del encierro forzado al desplazamiento ubicado, en el cual la persona vigilada no deja de encontrarse bajo la acción de un poder que ahora sobrepasa los límites de una barrera física para penetrar en prácticamente cualquier tipo de terreno y campo con su acción predatoria respecto al posicionamiento del sujeto detectable. Lo anterior es tan solo un ejemplo de la vasta multiplicidad de ingenios tecnológicos que se han multiplicado en época reciente cuya conformación y operatividad hacen proclive la extensión e intensificación de procedimientos de vigilancia, control y detección de alto poder. Se puede pensar desde el biochip, los circuitos y redes de video vigilancia, los controles biométricos, hasta las tecnologías GPS, pasando por toda la amplia y extendida gama de dispositivos, gadgets y redes que intensifican los efectos perniciosos invasivos de estas tecnologías, ahora extendibles a prácticamente cualquier rincón existente por debajo, sobre o en la tierra.

Lo anteriormente descrito se enlaza de manera definitiva con la presencia de un entramado y modalidades de socialización relacionadas a tipos de vigilancia contemporánea. Uno entre varios planteamientos que ejemplifican este tipo de posturas críticas respecto a la disposición y utilización de tecnologías destinadas a la vigilancia, la detección y el control, lo encontramos en el trabajo conjunto de Zygmunt Bauman y David Lyon titulado *Vigilancia líquida*. En dicho texto, los autores se dan a la tarea de reflexionar sobre las diversas condiciones de la vigilancia moderna, entre las cuales nos interesa destacar algunos aspectos. Una de las características fundamentales que Zygmunt Bauman y David Lyon identifican en la vigilancia

moderna asociada a las nuevas tecnologías de la información y la comunicación, es su carácter dúctil, móvil y flexible. Reconocen al propio Gilles Deleuze su postura pionera respecto a las sociedades de control que mencionamos anteriormente, para catapultar desde esta propuesta sus ideas respecto a la liquidez de la vigilancia. Ello quiere decir que los procedimientos actuales de vigilancia e identificación se han vuelto extremadamente flexibles, en contraposición con formas anteriores de control las cuales eran mucho más sólidas, macizas e inamovibles. Esta última idea la plantean teniendo en mente el modelo panóptico benthamiano, asociado a las disciplinas en una época donde estás prácticas de poder se fundamentaban en sólidos ingenios disciplinarios, caracterizados por la presencia de dispositivos de enclaustramiento para la examinación detallada de los seres humanos. Hoy día, en consonancia con la flexibilidad de relaciones sociales que se han vuelto mucho más móviles (al grado de observar ya no una sociedad, sino más bien, una red cuyos miembros se entienden a la manera de nódulos dispersos, tal como lo plantea el propio Zygmunt Bauman en su texto *La sociedad sitiada*) la tecnología aporta un insumo importante por cuanto al destino del control social mismo. Esta forma de vigilancia es coincidente con la composición de la sociedad líquida y flexible a la que alude Zygmunt Bauman ha hecho mención en diversas ocasiones. Sobre la conformación y operatividad de la vigilancia líquida podemos encontrar la siguiente afirmación:

> Gilles Deleuze introdujo la idea de «sociedad de control», en la que la vigilancia crece no tanto como un árbol –de manera relativamente rígida, en un plano vertical, como el diseño panóptico–, sino más bien como una planta trepadora. Cómo observaron Haggerty y Ericsson, y siguiendo la idea de Deleuze, el «entramado de vigilancia» captura flujos de lo que se podría llamar «un cuerpo de datos», convirtiéndolos en unos «datos dobles» altamente fluidos y móviles. William Staples también ha destacado que la vigilancia actual se produce en culturas «caracterizadas por la fragmentación y la in-

> certidumbre, en las que los sentidos tradicionales, los símbolos y las instituciones de la vida moderna se *disuelven* ante nosotros». Así, todos los vínculos, las estructuras y todo lo estable se vuelve líquido.[16]

Esto nos permite advertir una sentencia interesante e inquietante, puesto que los mecanismos actuales de control social destinados a la vigilancia, identificación y detección, se han refinado significativamente en función del contexto económico, social y político existente, de la mano de la creación de los nuevos ingenios tecnológicos comunicativos e informacionales que han potenciado, soportado, complementado y posibilitado, estas nuevas formas del control y la dominación social. La vigilancia post-panóptica a la que hacen alusión Zygmunt Bauman y David Lyon se presenta en un contexto definido por un alcance de poder indeterminado, puesto que la capacidad de filtración del mismo, vía las nuevas tecnologías de la comunicación y la información, se encuentra extendido a prácticamente todos los rincones de la vida pública y privada.

Precisamente sobre los alcances de estas tecnologías de control en la vida, encontramos afirmaciones como las realizadas por Paula Sibilia, quien en su obra *La intimidad como espectáculo*, nos advierte sobre el paulatino decaimiento de lo íntimo y el emergente fenómeno de lo éxtimo, como rasgo distintivo de nuestra época, en la cual se invierte la antigua práctica de la pastoral cristiana, lo que da por resultado que ahora en una sociedad vouyer y confesional, las mismas personas aperturan su intimidad, potenciando el alcance de las nuevas tecnologías a los rincones propios y particulares del ser humano, lo que de resultas hace que dichos datos queden expuestos a bases de datos y flujos de información. Por lo tanto, la vigilancia no solo se extiende a los espacios públicos, sino que se filtra a las redes informáticas mediante ese mismo fenómeno que Zygmunt Bauman y David Lyon denominan como escopofilia, es decir esa afición a ser visto, en el contexto de una sociedad donde exponerse, venderse y

16 Bauman, Zygnunt y Lyon, David, *Vigilancia líquida*, Paidós, Buenos Aires, 2017, pp. 11-12.

mostrarse, resultan en patrones de socialización que se han regularizado, como parte de los modos de vida de sus miembros-nódulos.

En un sentido similar, las afirmaciones planteadas por Byung Chul Han en sentido crítico expresan la aparición de la sociedad que él denomina de la transparencia, en la cual, paulatinamente, los espacios oscuros de anonimato y reserva (tan necesarios para el desarrollo de una vida social en la cual aquellos elementos negativos de ocultamiento y anonimato, hacen posible el balance y soporte con aquellos puntos de apertura y transparencia) van desapareciendo en contraposición de la afirmación de lo transparente, lo visible y lo identificable. Esta "positivización" de la vida, no se refiere al discurso pro democracia en el cual la accesibilidad a los datos se convierte en sinónimo evolutivo. Más bien, esa cobertura de puntos positivos de iluminación, esclarecimiento, transparencia y visibilidad del todo, se muestra como un dispositivo de control y poder que por múltiples vías se filtra hasta lo más íntimo de los resquicios sociales y de la vida individual, para tratar de mostrar, en un afán de control, cuáles son todos, absolutamente todos los aspectos de la vida de un ser humano que deben ahora ser escrutados y puestos en proyección para que su detección y control sea pleno. La pornografización por cuanto al acceso directo que respecto a nuestros ojos tiene la realidad y ese inclemente afán voyerista, hacen de la sociedad de la transparencia el lienzo perfecto para que los aspectos asociados a la vigilancia, suscritos y criticados por Zygmunt Bauman y David Lyon, se desarrollen de manera plena.

No resta más que señalar, por nuestra parte, la presencia de este tipo de ingenios destinados a la dominación social e individual (*omnes et singulatim* como bien lo refería Michel Foucault) con alto grado de precisión y efectividad, pues a la lógica panóptica (como Zygmunt Bauman y David Lyon bien refieren en su obra, echando mano de los planteamientos de Didier Bigo y Thomas Mathiesen) hoy día deben abonarse los referentes banópticos y sinópticos, que introducen una idea de totalidad respecto al alcance que estos me-

dios de la vigilancia detectiva establecen. El control socio-individual, vía las tecnologías, puesto sobre todos nosotros obedece a un afán no solo circunscrito al tema de la vigilancia, sino también a los de la categorización social por clase y procedencia, así como a la segmentación para la identificación, localización y detección de las personas en diversos contextos, útiles en dinámicas diversas, que abarcan desde los aspectos comerciales, hasta los propiamente secutitarios. Así, este poder se extiende de manera impresionante y absoluta hacia los diversos rincones de la vida humana, respecto del cual los puntos de oposición y contrapoder resultan indispensables para combatir esta lógica, donde la indetectabilidad se ha convertido en empresa de contraconducta.

III. OBSTACULIZACIÓN DEL CONTROL Y VIGILANCIA POR LAS TIC´S.

El control y la vigilancia de los individuos, de su existencia, dinámica y espacio-tiempo, por parte de un sujeto o grupos de sujetos para cualquier fin o interés solo es posible mediante el apoderamiento de los entornos de la realidad, de sus contextos, reglas, pautas y condiciones por las que se estructuran esquemas de pensamiento que facilitan interacciones de dominación entre individuos.

El apoderamiento de los escenarios de realidad, para el control y la vigilancia –la sujeción- de los individuos, se origina en la medida que las interacciones de la realidad forman vínculos de dominación, que se producen y reproducen por medio de los discursos de verdad, dirigidos a la normalización de las relaciones y la instrucción de las conductas de los individuos afectados e inmersos en la proyección de la realidad.[17] Si se desea el dominio de la realidad, será inevitable generar un control y vigilancia de los entornos donde esta se proyecta, desde el poder y la verdad como criterios que definen las interacciones de los sujetos.

17 *Cfr.* Foucault, Michel, *Poder, Derecho y verdad,* Segunda lección, 14 de enero de 1976, del curso en el College de France, París, 1975-76, publicando en: *Genealogía del Racismo, De la Piqueta, Madrid, 1992.*

De modo que, existe una relación necesaria dentro de la vigilancia y el control de los entornos donde se manifiesta la realidad: La Verdad y el Poder; esto es que, las múltiples y exponenciales interacciones de poder dentro de la realidad, solo pueden constituirse y conquistar el entorno, por vía de los discursos de verdad que se ligan indispensablemente a la transferencia del poder que generan los controles y la vigilancia de los individuos[18].

Tal relación de Verdad-Poder, no se contrapone a la realidad formada de manera intersubjetiva por símbolos significantes para los individuos; poder, verdad y realidad, no son categorías excluyentes entre sí: la realidad no suprime a la verdad y viceversa. Por otro lado, la realidad necesariamente experimenta la conformación del poder, se modifica o perpetúa acorde a la economía de la verdad y las relaciones de poder.

Se ha señalado que, la realidad es un proceso mental fijado y proyectado desde la inteligencia, empero la verdad, su economía y el poder, refieren a un proceso derivado de las múltiples interacciones de los sujetos dentro de los entornos de realidad, por medio del cual los detentadores del poder, se apropian y conquistan las pautas o reglas, así como las estructuras de pensamiento de la realidad para ser establecidas como certezas, verdades propias del medio; evitando con esto que diversas representaciones de la realidad puedan manifestarse, o bien, se manifiesten conforme a los criterios, pautas, reglas o lineamientos de los discursos de verdad.[19]

La verdad se verifica como un filtro para la inteligencia y la pro-

18 Dentro del texto *Poder, derecho y verdad, Óp. cit.*, p. 84, el propio Michel Foucault puntualiza lo siguiente sobre este particular: "No hay ejercicio del poder posible sin una cierta economía de los discursos de verdad que funcione en, a partir de, y a través de este círculo: estamos sometidos a la producción de la verdad del poder y no podemos ejercer el poder sino a través de la producción de verdad."

19 "Estamos sometidos a la verdad también en el sentido de que la verdad hace ley, produce el discurso verdadero que al menos en parte decide, transmite, lleva adelante el mismo efecto de poder. Después de todo, somos juzgados, condenados, clasificados, obligados a deberes, destinados a cierto modo de vivir o de morir en función de los discursos de verdaderos que comparten efectos específicos de poder". *Ibidem.*, p. 85.

yección de la realidad en el entorno; todo esto, en una relación de coexistencia que directa y recíprocamente afecta a ambos aspectos: Verdad y Realidad. La verdad configura determinadas realidades, la realidad proyectada desde la mente configura verdades. La confiscación del entorno de la realidad, por los sujetos que detentan el poder, especifica pautas de conducta y reglas de interacción, para codificar de manera determinada los elementos que configurarán la realidad en el proceso de inteligencia, de igual forma, para ser proyectada bajo lenguajes y rutinas fijadas por la verdad, en el entorno.

Clarificando el discurso, el poder y la verdad como relación necesaria para la dominación y el apoderamiento, para el control y la vigilancia de los sujetos en los entornos de la realidad, establece reglas de interacción, pautas de manifestación de la realidad, ora para la normalización de los sujetos, ora para su tasación, ora para su verificación; que desde tales regulaciones la apropiación de los entornos, es factible en un grado mayor, por la dominación de los sujetos sobre los sujetos y su existencia.

Lo dicho hasta aquí, puede suponer una realidad rígida bajo modelos y cánones preestablecidos, inmutable en cuanto se conservan las relaciones de poder que originan a las pautas y reglas de los entornos de la realidad; sin embargo atendiendo al "proceso de licuefacción", al "derretimiento de los sólidos" que implica el paso a la liquidez de la modernidad, las pautas o reglas de la realidad sujetas a la tradición, a lo sagrado como armadura de lo solido son negadas en el tiempo, en su historia y pasado, para disiparse y emanciparse de todo aquello que obstaculiza su liquidez o cambio constante.[20]

En consecuencia, bajo los aspectos de la modernidad líquida, las pautas o modelos de la realidad son despojados de un poder coercitivo, por la falta de determinación, evidencia y el sobre cúmulo de

20 "Si el 'espíritu' era 'moderno', lo era en tanto estaba decidido a que la realidad se emancipara de la 'mano muerta' de su propia historia… y eso solo podría lograrse derritiendo los sólidos (es decir, según la definición, disolviendo todo aquello que persiste en el tiempo y que es indiferente a su paso e inmune a su fluir)". Bauman, Zygnunt, *Modernidad Líquida*, Fondo de Cultura Económica, Argentina, 2004, p. 9.

configuraciones, que se contradicen o colisionan entre sí: con ello, la liquidez, entrega al individuo la responsabilidad de creación de modelos de interacción que permitan construir, moldear o manipular de forma flexible, poco previsible y fluida la realidad que lo rodea, las relaciones de poder que lo proyectan y reconocen en un espacio y tiempo desvinculados.[21]

La desvinculación del espacio y el tiempo como esencia de la modernidad, transforma necesariamente las relaciones de poder y la generación de pautas y reglas de la realidad; el tiempo moderno como fluido y con capacidad de contención, conquista el espacio sólido, a razón de la velocidad en el movimiento entendida como un recurso humano, como un ingenio en el desplazamiento del poder. El avance tecnológico, implicado a la modernidad, y a la conquista del tiempo sobre el espacio, permite romper los límites sólidos de contención del movimiento, consolidándose como instrumentos principales del poder y la dominación, que se expresa de manera extraterritorial e instantánea.[22]

Así las formas de apoderamiento de los entornos de la realidad para el control y la vigilancia de los sujetos, bajo la generación de estructuras de pensamiento, pautas y modelos desde las interacciones que transmiten y difunden el poder, se observa trastocada por la modernidad liquida y los medios tecnológicos, que representan la construcción de un entorno virtual, una proyección existencial de la sociedad y los individuos, enmarcada bajo las relaciones de inteligencia Humana, Tecnologías de la Información y Comunicación, así como de una Inteligencia Artificial, que opera e integra bajo un lenguaje Máquina-Sujeto, una dimensión con tiempo flexible y sin obstáculos espaciales.

Conforme a lo expresado, es posible establecer la apropiación del entorno virtual para el control y la vigilancia empleando los

---

21 Cfr. Bauman, Zygmunt, *Modernidad líquida*. México. Fondo de Cultura Económica 2003.

22 *Cfr. Idem*.

medios tecnológicos disponibles atendiendo a fines e intereses particulares o privados; tal apropiación o conquista no se realiza sobre los sujetos, menos aún sobre los espacios de un entorno virtual; sino sobre la información que se transmite, difunde y manipula en el entorno, así como sobre el tiempo que se expresa por la velocidad de transmisión de la información y la capacidad de almacenar los datos en una historia de un presente constante.

Lo anterior afirma que, la verdad, sus discursos y el poder no se expresan dentro del entorno virtual por la generación esencial de pautas o normas que regulan o controlan las interacciones físicas de los individuos, es decir la sujeción y vigilancia de los cuerpos; sino por la conformación de justificaciones más o menos racionales para el dominio de la información, que fluye de manera constante en la virtualidad.

De suerte que, si la conquista del entorno artificial corresponde al apoderamiento y uso de la información, que fluye de manera constante por mecanismos y medios tecnológicos de acceso general para todos los individuos, su ocupación total y plena con los fines de control y vigilancia, se verifica de manera parcial. Entendido que, en toda interacción y transferencia del poder, dentro de la realidad, existe una resistencia, así como posibilidad de emplear y ejercer el poder que se transmite; en caso particular, la información que expande y fluye en el entorno digital, posibilita a cualquier sujeto a apoderarse de una parte mínima del entorno, así como oponerse a los mecanismos de control y vigilancia de la información, por vía de la misma información.[23]

En esa línea discursiva, el entorno virtual de la realidad escapa de la relación sólida o estática de dominante y dominando, en la dimensión que aquello sobre lo que se pretende controlar y vigilar, es

23 "En la medida en que el sistema viral de la lengua se reproduce con gran facilidad y condiciona toda actividad humana, el *virus -palabra* y su difusión más mediática puede volverse tanto instrumento de control y sujeción mental, como un arma destinada a sabotear y anular esos mecanismos". Burroughs, William S., *La Revolución Electrónica,* Editorial Bruguera, Barcelona España, 1993, p. 12.

producto parcialmente de una inteligencia artificial, ajena al sujeto mismo, que realiza procesos de interacción independientes a los individuos, a su existencia material y de pensamiento, bajo lenguajes máquina -binarios-. Una inteligencia máquina, que permite la interfaz sujeto-tecnología digital, que se configura por la cantidad de nodos de TIC´s activos o inactivos que transmiten y difunden la información más allá de la existencia de los sujetos, como elemento esencial para el entorno virtual, dentro de una red continuamente activa.

Considerando ahora que, sobre la probabilidad latente de apoderamiento de la información, que cada sujeto representa en el entorno digital, al emplear de forma activa o pasiva las Tecnologías de la Información-Comunicación y que las interacciones de poder dentro de la virtualidad se desplazan sobre un espacio amplio sin límite sólido o natural, generando relaciones liquidas de control y vigilancia sobre los datos que se almacenan, distribuyen y manipulan; entonces, la principal técnica para el ejercicio del poder y para su resistencia dentro del medio digital, es la huida, el escurrimiento; es decir, evitar la detección en el entorno, para desplazarse dentro del mismo de forma informática, libre y anónima, sin obstáculos que impliquen la posibilidad de sujeción, o construcción de un orden sólido.[24]

El individuo inmerso en la modernidad liquida, carga consigo la responsabilidad de construir su identidad, una autoconstrucción desde bases genéricas y modelos efímeros y flexibles puestos en el mercado para su adquisición, que no respetan orden o límites jerárquicos. Los sujetos se encuentran vagando entre la responsabilidad de construirse a sí mismos y la tarea de huir de cualquier carga o peso que les impida fluir en la liquidez de la modernidad; por lo

24 La principal técnica de poder es ahora la huida, el escurrimiento, la elisión, la capacidad de evitar, el rechazo concreto de cualquier confinamiento territorial y de sus engorrosos corolarios de construcción y mantenimiento de un orden, de la responsabilidad por sus consecuencias y de la necesidad de afrontar sus costros". Bauman, Zygnunt, *Modernidad Líquida, Óp. Cit.,* p. 17.

que, tal contradicción es resuelta mediante la generación de identidades pasajeras y remplazables que puedan dejarse de lado cuando sea necesario conforme a sus intereses, o bien, cuando se pretende la sujeción a construcciones rígidas para la vigilancia y el control.[25]

Precisando, los sujetos se desplazan e interaccionan dentro de la modernidad, por vía de una identidad que es entendida como un conjunto de pertenencia que se ensambla a una unidad básica o un cimiento genérico otorgado al sujeto por el mercado que rige las pautas o reglas de la realidad. Por lo que hace a la realidad digital, la identidad es generada por la información de los individuos que se expone en el medio a través de las TIC's, donde se crean múltiples copias de datos de pertenencia que se almacenan y manipulan en la inteligencia artificial; el "yo" virtual de los sujetos es una dimensión más de la identidad de los individuos proyectada en información dentro de la virtualidad.

La identidad virtual, como dimensión de los sujetos, no representa una fragmentación de la construcción realizada en distintos entornos de la realidad, sino un aspecto fraguado en parte o en totalidad por los sujetos, a través de los instrumentos tecnológicos; una multi-dimensión que se expone por la combinación de herramientas técnicas materiales -*Hardware*- , técnicas lógicas -*Software*- y la inteligencia humana, que prolonga la existencia del sujeto y sus interacciones a un entorno netamente informático, abstracto y a un tiempo histórico en la medida de la capacidad de almacenamiento digital.[26]

Entendiendo al "yo" virtual, como una dimensión de la identidad, que se construye de manera flexible y pasajera por un conjunto de pertenencias y que se proyecta por medio de la información en

---

25 *Cfr*. Bauman, Zygmunt, *Modernidad líquida*. *Idem*.

26 *Cfr.* Sánchez Martínez, José Alberto, *La Comunicación sin cuerpo. Identidad y Virtualidad*, Revista Méxicana de Ciencias Políticas y Sociales, volumen 52, no 209, Universidad Nacional Autónoma de México, México, 2010, obtenido en: http://www.revistas.unam.mx/index.php/rmcpys/article/view/25962 consultado: 22 de mayo de 2020.

el ambiente digital; es asequible afirmar que todo sujeto que accede a la virtualidad se encuentra posibilitado para generar diversas dimensiones de su identidad, que se multiplican exponencialmente por las copias que de su información se generan al interaccionar con los sujetos y la memoria artificial, todo en tiempo real. Lo anterior quiere decir que, un solo individuo, puede generar dos o más dimensiones de su identidad en el entorno, sea por manifestar en él parcialidades de información, esto es, ocultar datos de identificación o pertenecía; o bien, por falsear parcial o totalmente la información de su identidad, y construir con ello una dimensión diversa de su identidad.

Más aún, al multiplicarse las interacciones en el medio, la inteligencia artificial, genera copias de los datos de identidad que se han revelado dentro del entorno, con ello se posibilita la extensión de existencia de las dimensiones de la identidad de los sujetos, manifestada parcial o en nueva y diversa construcción; las múltiples copias de identidad, como toda la información en el espacio digital, fluyen de manera constante entre los nodos de la red, donde es recibida y decodificada para su aprehensión por sujetos o herramientas de información, lo que permite el reconocimiento de pertenencia de la identidad del sujeto.

El reconocimiento del "yo virtual" -identidad parcial o construcción diversa- o de sus copias digitales, por parte de los sujetos dentro del entorno o de la inteligencia artificial, estructura una coexistencia en tiempo único de la información de un solo sujeto, que puede o no estar ejecutando acción en el entorno digital. La posibilidad de dimensionar la identidad de forma múltiple y el reconocimiento del entorno de las copias de información de un sujeto, apertura la técnica de la huida, del anonimato, para el ejercicio o resistencia al poder, así como a los mecanismos de control y vigilancia que emplean las tecnologías de la Información y Comunicación.

Construir, ocultar o falsear datos de identidad, así como la lejanía de la comunicación y su celeridad, hacen factible el anonimato visual,

por no garantizar que el sujeto fuera del entorno refleje fielmente la información que proyecta en el espacio digital; los individuos pueden modificar, manipular y construir una dimensión de identidad, conforme a su voluntad e intereses. Una identidad a voluntad otorga el potencial de desinhibirse, de mostrar parte de la identidad que se oculta en otros contextos de realidad donde la presencia o contacto físico es necesario para la interacción de individuos, ello con la finalidad de explorar diversos roles o personalidades, para intereses polimorfos e individuales.[27]

En síntesis, debe asimilarse que si bien, la información que fluye en la virtualidad, puede exponer al sujeto a técnicas de control y vigilancia eficientes, por adentrarse a los aspectos últimos de su privacidad, al resquicio oculto de su vida social, en la medida que la identidad se hace más transparente, visible y pornográfica -en el sentido de una visualización inmediata, directa y explicita- por el constante manejo, manipulación y empleo de las TIC's que permiten la detección e identificación de los sujetos en tiempo real, así como en todos los aspectos de la vida pública o privada como un poder indeterminado y extraterritorial; lo es también, que el exceso de información dentro del entorno, la multiplicidad de identidades y la posibilidad del anonimato, permiten la contraposición a la vigilancia y el control de los sujetos; la virtualidad, entendida bajo aspectos de flexibilidad y liquidez, imposibilitan la conquista plena del medio, y con ello el establecimiento total de pautas o reglas que permitan la detección y sujeción de los individuos. En un entorno donde se puede jugar con la existencia y el ingenio es la herramienta principal, ningún límite es viable.

---

27 Cáceres Zapatero, María Dolores, "Sociabilidad virtual: la interacción social en el ecosistema digital", contenido en *Revista Historia y Comunicación Social*, vol. 22, no. 1, pp. 233-247, Universidad Complutense de Madrid y Universidad de Murcia, Madrid, 2017.

IV. EPÍLOGO. FUNCIONALIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN LA POLÍTICA CRIMINAL.

En el contexto de la modernidad, a los procesos de dominación de los cuerpos de los sujetos, la gestión de los fenómenos de natalidad y mortalidad en las poblaciones debe sumarse la apropiación de la información del espectro digital de los individuos, como un dispositivo complejo de control y vigilancia. Es decir, a la lógica del biopoder empleada bajo mecanismos y pautas anatomopolíticas y biopolíticas, para la sujeción de los individuos, es necesario adherir, bajo el tejido de la ruptura de los paradigmas del espacio y el tiempo, de la liquidad de la sociedad, así como de las relaciones, el uso de la psicopolítica[28], entendida como la apropiación de la información o datos inmersos en el medio digital.

Las tecnologías de la información y comunicación transmutan tanto el cuerpo físico como el conjunto social, a lenguaje máquina o datos, que permitan la interacción en el campo virtual de la realidad; el sujeto existe de forma física detrás del ordenador o el dispositivo móvil de comunicación, y de forma virtual por medio de datos: Identificaciones digitales, en el contexto de la realidad simulada. El sujeto, se autoidentifica en el mundo digital, se relaciona en información de forma pornográfica, en un entorno constante sin limitaciones espacio temporales; en consecuencia, se entrega o sujeta de forma libre a un poder seductor[29], con la finalidad de ser insertado a las relaciones de dominación psíquicas.

De tal suerte que, la información que se entrega o se inserta de forma libre dentro de la realidad virtual, es empleada para la identificación psíquica de los sujetos, así como para la predicción de sus acciones dentro del creciente consumismo que impone la modernidad liquida; en ese sentido el control y la vigilancia se desarrolla de

---

28 *Cfr*. Han, Byun-Chul, *Psicopolítica: Neoloberalismo y nuevas técnicas de poder*, Herder, Barcelona, 2014.

29 *Cfr*. *Idem*.

forma permanente, tanto por quien o quienes emplean las tecnologías de la información como por la inteligencia artificial, que procesa, almacena y distribuye los datos dentro de la red informática.

Ahora bien, la Política Criminal no escapa a la lógica del poder, sea por la dominación de los cuerpos, las poblaciones, o bien la psique de los sujetos; todo ello, con la finalidad de controlar y vigilar procesos anómicos, que incidan en el mantenimiento y permanencia de las estructuras sociales y estatales. El uso de las TIC´S dentro de la Política Criminal no se expresa aquí como un elemento novedoso, ejemplo de esto resalta la "Policía Cibernética" o los "Ciber Delitos"; el primer elemento, refiere a la Política Criminal en sentido estricto, siendo la policía uno de los operadores del sistema penal en la prevención de la criminalidad; mientras que la segunda referencia alude a la Política Criminal en sentido amplio, de forma concreta a la construcción o establecimiento de las conductas definidas como delitos.

El eje central de la redacción expresa, que no siendo un elemento novedoso el uso de la tecnología en la Política Criminal es necesario preguntar ¿Qué grado de funcionalidad o eficacia, tienen las TIC´S en el control y vigilancia de los procesos anómicos dentro de la sociedad? ¿Obstaculizan o posibilitan la detección de personas? ¿Previenen o potencializan la comisión de -nuevos- delitos?

Como se ha presentado, el poder que se liga a la apropiación de la información dentro de la realidad virtual potencializa la identificación, clasificación o detección de sujetos y a su vez el anonimato o el ocultamiento, ambos fenómenos derivados de la multiplicidad de datos que fluyen en dicho entorno cuyos filtros se presentan laxos. El ambiente digital, se expresa así, como el campo de cultivo, para la comisión de nuevos delitos -digitales-, y una herramienta para la ejecución de conductas tipificadas anteriormente.

Habría que señalar también, que la realidad social de los individuos se construye en lo cotidiano de estos, en la percepción sensorial del momento, bajo las circunstancias sociales, económicas y

políticas en las que se encuentran; y es ahí, en lo próximo, en el hacer cotidiano, que el uso de las TIC´S, que el sumergirse a la virtualidad, se ha colocado en una necesidad, en un medio para relacionarse y reconocerse. El 'yo' individual, la percepción de mi existencia e identidad, no solo se desdobla en un 'yo-social', sino también en un 'yo-virtual'.

El fenómeno anómico, la criminalidad, no escapan de esta nueva realidad cotidiana, sino que también se adaptan y desdoblan como procesos sociales, en la virtualidad; las expresiones de la política, el poder y la vigilancia, encontraran también sus homólogos dentro de ambiente digital, bajo las pautas y reglas que se permitan. Como es afuera es adentro, la edificación de los medios y del entorno, son producto del razonamiento humano, y por tanto falibles en su lógica y su estructura.

De forma concreta, es funcional el uso de las TIC'S en la Política Criminal, en la medida en que la lógica del poder utilizada en los mecanismos de vigilancia y control requiera la identificación, detección y clasificación, de sujetos, conductas o procesos; sin obviar que en todo uso del poder, siempre existirá una resistencia al mismo, que empleara los mismos medios, en forma inversa, es decir, para el ocultamiento, el anonimato y sobre todo, para el desequilibrio de las estructuras que hubiesen dado origen al acto de poder primigenio.

Tanto la anatomopolítica, como la biopolítica y la psicopolítica, tienden a la dominación de los fenómenos existenciales sea poblacionales o sea de los individuos; el Ser y Estar en un tiempo y espacio determinado, convierte a las personas en agentes susceptibles de ser construido, apropiado o dominado.

La Política Criminal, en su lógica básica, implica el control de dichos fenómenos, la intromisión mínima en el 'yo' de los sujetos, quienes representan un potencial latente de anomalidades, de peligros mediatos a las estructuras de poder; la prevención, la construcción y el tratamiento del crimen, dentro de la realidad virtual,

solo es visible bajo la justificación del riesgo a bienes jurídicamente tutelados -intereses económicos o políticos-. En otras palabras, el control y la vigilancia dentro de la realidad virtual, como fuera obedece a las relaciones de poder y los detentadores de este.

V. FUENTES DE INFORMACIÓN

Bibliografía

Bauman, Zygmunt, *La sociedad sitiada*, Fondo de Cultura Económica, México, 2011.

_____ Lyon, David, *Vigilancia líquida*, Paidós, Buenos Aires, 2017.

_____, *Modernidad Líquida*, Fondo de Cultura Económica, Argentina, 2004.

Berger, Peter L., Luckman, Thomas, *La construcción social de la realidad*, Amorortu Editores, Buenos Aires, Argentina, 1999.

Eco, Humberto, *Apocalípticos e integrados*, Editorial Lumen, España, 1984.

Foucault, Michel, *Genealogía del Racismo*, De la Piqueta, Madrid, 1992.

Han, Byun-Chul, *Psicopolítica: Neoloberalismo y nuevas técnicas de poder*, Herder, Barcelona, 2014.

Reyes Echeagaray, Dora Alicia, *Tecnologías de Información y comunicación en las Organizaciones*, Facultad de Contaduría y Administración, Publicaciones Empresariales UNAM, FCA Publishing, Ciudad Universitaria, México, 2015.

Hemerografía

Cáceres Zapatero, María Dolores, "Sociabilidad virtual: la interacción social en el ecosistema digital". *Revista Historia y Comunicación Social*, vol. 22, no. 1, pp. 233-247, Universidad Complutense de Madrid y Universidad de Murcia, Madrid, 2017.

Heras Lara, Lizbeth y Villarreal Benítez José Luis, "La realidad virtual en los nuevos paradigmas de la ciencia de datos". *Revista Digital Universitaria*, Volumen 12, Número 9, Coordinación de Acervos Digitales,

Dirección General de Cómputo y de Tecnologías de Información y comunicación, UNAM, 1 de septiembre 2011.

Villamizar, Gustavo y DONOSO, Roberto, "Definiciones sobre inteligencia. Revisión histórica". *Psicogente*, 16 (30), Julio-Diciembre, Universidad Simón Bolívar. Barranquilla, Colombia, 2013.

Cibergrafía

Bravo Ramírez, Leticia, et al, *Análisis de las tecnologías de la información y de la comunicación (TIC'S) en México*, obtenido en: www.paginaspersonales.unam.mx consultado: 5 de junio de 2019.

Deleuze, Gilles. *Posdata sobre las sociedades de control*, obtenido en: https://www.fundacion.uocra.org/documentos/recursos/articulos/Posdata-sobre-las-sociedades-de-control.pdf consultado: 12 de noviembre de 2019.

Fabres Barahona, Juan Carlos et al., Análisis del uso de las Tecnologías de la Información y la Comunicación en los establecimientos educacionales de Chile: Caso del Colegio Santo Tomás de la Comuna de Ñuñoa, Seminario para optar al Título Profesional de Ingeniero Comercial mención Administrativa, Universidad de Chile, Santiago de Chile, 2014, obtenido en: http://repositorio.uchile.cl/handle/2250/116586 consultado: 6 de junio de 2019.

Sánchez Martínez, José Alberto, "La Comunicación sin cuerpo. Identidad y Virtualidad", *Revista Mexicana de Ciencias Políticas y Sociales*, volumen 52, no 209, Universidad Nacional Autónoma de México, México, 2010, obtenido en: http://www.revistas.unam.mx/index.php/rmcpys/article/view/25962 consultado: 22 de mayo de 2020.

UNAM POSGRADO

Derecho

9 786073 046824