Universidad Andina Simón Bolívar

Sede Ecuador

Área de Estudios Sociales y Globales

Maestría en Relaciones Internacionales

Desafíos globales del cibercrimen

Caso Ecuador período 2014 – 2019

Alexandra Catalina Ochoa Marcillo

Tutor: Wolf Diether Grabendorff

Quito, 2021

Cláusula de cesión de derecho de publicación

Yo, Alexandra Catalina Ochoa Marcillo, autora de la tesis titulada "Desafíos globales del cibercrimen. Caso Ecuador período 2014 – 2019", mediante el presente documento dejo constancia de que la obra es de mi exclusiva autoría y producción, que la he elaborado para cumplir con uno de los requisitos previos para la obtención del título de Magíster en Relaciones Internacionales en la Universidad Andina Simón Bolívar, Sede Ecuador.

1. Cedo a la Universidad Andina Simón Bolívar, Sede Ecuador, los derechos exclusivos de reproducción, comunicación pública, distribución y divulgación, durante 36 meses a partir de mi graduación, pudiendo por lo tanto la Universidad, utilizar y usar esta obra por cualquier medio conocido o por conocer, siempre y cuando no se lo haga para obtener beneficio económico. Esta autorización incluye la reproducción total o parcial en los formatos virtual, electrónico, digital, óptico, como usos en red local y en internet.
2. Declaro que en caso de presentarse cualquier reclamación de parte de terceros respecto de los derechos de autor/a de la obra antes referida, yo asumiré toda responsabilidad frente a terceros y a la Universidad.
3. En esta fecha entrego a la Secretaría General, el ejemplar respectivo y sus anexos en formato impreso y digital o electrónico.

18 de febrero de 2021

Firma: _____

Resumen

Al mismo tiempo que avanzan las tecnologías de la información y la comunicación, los delitos informáticos o el cibercrimen toman sofisticadas y avanzadas formas de vulnerar el espacio cibernético y con ello cometer actos ilícitos sin ser fácilmente detectados; convirtiéndose en verdaderos desafíos globales para todos los países del mundo. En el caso de Ecuador, esta situación resulta ser un tema complejo en cuanto a la capacidad estatal, la formulación de políticas en ciberseguridad y la toma de decisiones para la regulación y tratamiento del cibercrimen.

El objetivo principal de esta investigación es examinar justamente los desafíos globales resultantes del ciberdelito, en particular para la legislación latinoamericana y las políticas para combatirlo. Por ello, en el capítulo primero se realiza una aproximación teórica del cibercrimen y su tipología, los desafíos globales para el mercado y para el Estado, y los esfuerzos de implementación de medidas de ciberseguridad para ambos sectores.

En el capítulo segundo se revisan los instrumentos internacionales en el tratamiento del cibercrimen y se realiza una breve comparación legislativa en Latinoamérica para aterrizar en el contexto ecuatoriano. Finalmente, en el capítulo tercero se exponen y analizan los casos relacionados a Julian Assange, Ola Bini y el robo de datos personales de los ecuatorianos en 2019.

Palabras clave: Desafíos globales, cibercrimen, políticas en ciberseguridad, capacidad estatal, actores no estatales

Esta investigación dedico principalmente a mi Eve, mi mayor consejera y persona favorita;
a mis padres quienes me han llevado a ser la mujer que soy hoy;
a mis hermanos que me han acompañado en este camino que se llama vida;
a mis amigos que me apoyaron en la consecución de este proyecto académico.

Agradecimientos

Nunca encuentro las palabras exactas para agradecer a todas las personas que me han acompañado durante cada etapa de mi vida. En especial, esta etapa académica en el que culmino muy agradecida por todos los momentos y espacios de conocimiento y autoaprendizaje, de todas las personas que pude conocer y las buenas conversaciones que tuve a lo largo de esta maestría.

Agradezco a ese ser omnipresente y sabio que me ha permitido vivir todas estas experiencias de vida y académicas.

A mis sabios padres, Rebeca Marcillo y Carlos Ochoa, quienes me han apoyado en cada meta que me he atrevido a soñar, y hoy, continúan a mi lado dándome fuerzas para alcanzarlas.

A mi Eve, mi hermosa hija que me ha regalado la vida, y me siento bendecida de estar a su lado.

A mi tutor Wolf Grabendorff, siempre pendiente del desarrollo de este proyecto y que agradezco culminar exitosamente.

A mi Napo, mi fiel amigo.

A todos los que me acompañaron, muchas gracias.

Tabla de contenidos

Abreviaturas

APCoC	Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems / Protocolo Adicional de la Convención en Cibercrimen relacionado con actos de xenofobia y racismo difundidos por medios tecnológicos
BID	Banco Interamericano de Desarrollo
CNT	Compañía Nacional de Telecomunicaciones
COE	Comité de Operaciones de Emergencia
COIP	Código Orgánico Integral Penal
COMJIB	Conferencia de Ministros de Justicia de los Países Iberoamericanos
COPLUTIC	Comité Plurinacional de Tecnologías de Información y Comunicación –
CSIRT	Computer Security Incident Response Team / Equipos de Respuesta a Incidentes de Seguridad Informática
FISC	Foreign Intelligence Surveillance Court / Ley de Vigilancia de la Inteligencia Extranjera
GAO	Government Accountability Office / Contraloría General del Estados Unidos
ICG	Índice de Ciberseguridad Global
OEA	Organización de Estados Americanos
OMC	Organización Mundial de Comercio
ONU	Organización de Naciones Unidas
SATJE	Sistema Automático de Trámite Judicial Ecuatoriano
SENAIN	Secretaría Nacional de Inteligencia
SOC	Security Operation Center / Centro de Seguridad
TIC'S	Tecnologías de la Información y la Comunicación
UIT	Unión Internacional de Telecomunicaciones
UNTOC	Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional

Introducción

El cibercrimen es un concepto ampliamente discutido por diferentes enfoques teóricos y técnicos, como el derecho, la criminología, la informática, la sociología y diversos análisis que han tratado de definirlo en categorías como el delito transnacional, el ciberespacio, ciberseguridad y la sociedad de la información. Es un fenómeno social global que avanza con gran rapidez al mismo tiempo que las tecnologías de la información y precisamente por sus desafíos globales han derivado en discusiones académicas alrededor de los temas de identificación, jurisdicción, regulación y tratamiento (Chawki et al. 2015, 22).

Dada la complejidad del ciberdelito, éste no puede ser abordado desde un solo punto de vista, sino desde varias perspectivas teóricas que permitan definir sus características, sus factores y por tanto a buscar soluciones para enfrentar este fenómeno global. Sin embargo, interesa estudiar el ciberdelito desde la perspectiva de las relaciones internacionales, un campo de análisis que permite comprender la globalidad de las dinámicas del ciberdelito y las redes del crimen transnacional que operan en diferentes esferas público-privadas, locales e internacionales y a través de diversos medios (digitales, tradicionales, materiales).

En términos doctrinarios, la legislación sobre el cibercrimen ha planteado cuestiones sobre los límites y la interacción entre la regulación interna y la normativa internacional de regulación y control del uso del internet. Pues, debido al carácter transnacional del ciberdelito, se presentan escenarios que rebasan la jurisdicción interna, dificultando la cooperación para detectar a los posibles autores. La mayor virtud del internet es precisamente "reducir al máximo posible las restricciones de su acceso y uso" (Albán 2016, 25).

En este sentido, se parte del estudio de los investigadores norteamericanos Thomas Holt y Adam Bossler (2016), quienes explican que el cibercrimen ha ido evolucionando en conjunto con los cambios de patrones sociales y el uso de nuevas tecnologías, y tratar de definirlo desde una sola perspectiva teórica resultaría inadecuado. Por ello, se recurre a un análisis global desde las corrientes crimonológicas hasta examinar las nuevas discusiones

alrededor de teorías específicas del ciberdelito que aborden y expliquen las características únicas del ciberespacio y la tecnología.

En conjunto con esta perspectiva, este estudio no solo explora las definiciones de la criminalidad también hace una revisión de las nociones jurídicas y las políticas criminales. Un punto que resulta necesario para comprender las legislaciones nacionales e internacionales para enfrentar a las formas de ciberdelito, que no solo traspasan las fronteras a través del ciberespacio, sino que también pueden formar parte de organizaciones criminales convirtiéndose en un problema transnacional. De esta manera, se realiza un análisis del concepto de criminalidad organizada transnacional donde se debaten las definiciones de delito internacional versus delito transnacional.

Se entiende por delito internacional aquel acto ilícito que viola únicamente el derecho internacional en el que varias naciones se ven afectadas, en cambio, el crimen transnacional a más de lesionar ”bienes jurídicos comunes de varios Estados” viola también su derecho nacional (Zúniga, 2016, 77)[1]. El crimen transnacional se ubica prácticamente dentro de las estructuras del crimen organizado, donde es más compleja la identificación de actores estatales, no estales u organizaciones. La diferencia de estos términos radica en el manejo propio de cada legislación nacional que determine si hay una violación a su juridicción nacional y que pueda afectar a otros Estados, como por ejemplo el uso y tráfico de armas o la trata de personas.

A partir de estas últimas definiciones es importante identificar el crimen transnacional desde la participación de actores privados y el crimen internacional por actores estatales. Pues la naturaleza de los actores son los que definen los alcances y motivos del cometimiento de los diferentes delitos informáticos. Por tanto, una de las aristas a tratar en esta investigación es la de identificar, al menos teóricamente, qué actores existen, cuáles son sus fines (políticos, financieros) y qué normativa mitiga sus acciones.

Los desafíos globales que enfrentan los distintos países del mundo han llevado a la planificación y ejecución de políticas en ciberseguridad y criminales. Sin embargo, las respuestas del Estado frente a estos desafío han sido mínimos, pues dependerá de la

[1] En los casos de delito internacional se pueden encontrar violaciones a los derechos humanos, crímenes de guerra, crímenes de lesa humanidad, genocidio. Son los delitos condenados internacionalmente bajo el derecho penal internacional. Los casos de delito transnacional son aquellos que violan tanto la legislación nacional como internacional como por ejemplo la trata de personas, el narcotráfico, tráfico y uso de armas.

capacidad estatal para resolver los delitos informáticos y del desarrollo de instrumentos de cooperación internacional que permitan operar en distintos esferas y niveles nacionales, internacionales o transnacionales.

Frente a este contexto, los países se han centrado principalmente por mejorar e implementar medidas de seguridad informáticas como la protección a datos públicos, especialmente por la afectación a sus instituciones estatales. Según el Índice de Ciberseguridad Global (ICG, 2018), realizado por la Unión Internacional de Telecomunicaciones (UIT) que mide indicadores basados en los niveles de seguridad y protección de datos públicos y privados de varios países del mundo en una escala de 0 a 1. Los países que lideran esta ranking son países desarrollados como Reino Unido (0.93), Estados Unidos (0.92) y Francia (0.91). En los primeros lugares de América Latina, Uruguay ocupa la posición 51 con 0.68 puntos, México posición 63 con 0.62, Paraguay posición 66 con 0.60, mientras que Ecuador en la posición 98 con 0.36 puntos.

Para el caso de Ecuador, en materia de ciberseguridad, apenas en 2018 inició una consultoría para la "Elaboración de la Estrategia Nacional de Ciberguridad" impulsada por el Ministerio de Telecomunicaciones y la Sociedad de la Información para la protección de datos e información gubernamental (MINTEL, 2019) y una Ley de Protección de Datos que aún se debate en la Asamblea Nacional desde el 2019.

Con estos antecedentes, es necesario identificar ¿cuáles son los desafíos globales resultantes del ciberdelito, en particular para las legislaciones latinoamericanas, caso Ecuador y cuáles son las políticas para combatirlo?

Un planteamiento que se resolverá a lo largo de esta investigación a través del análisis de las definiciones conceptuales de ciberdelito, la comparación legislativa de los países latinoamericanos resaltando específicamente los desafíos globales y que plantea el ciberdelito, y el análisis de los casos de J. Assange, Ola Bini y del robo de datos de los ecuatorianos en 2019.

Casos que permiten dimensionar los desafíos globales, los alcances políticos e incluso el juego de intereses que pueden formar parte de la comprensión, tratamiento y regulación del cibercrimen en Ecuador.

Capítulo primero
Aproximaciones teóricas del ciberdelito

1. Definición del cibercrimen

El ciberdelito o en su término anglosajón *cybercrime*, es un concepto que evoluciona junto con las nuevas tecnologías de la información y de la comunicación, al mismo tiempo que las actuales generaciones han ido modificando sus formas de pensamiento y de conducta humana, el delito tiene una nueva concepción. El delito no solo ha cambiado de lugar hacia el ciberespacio, se ha tornado en un concepto discutido por diferentes estudios, que al ingresar al internet, se transforma en una zona gris que pone en debate los principios tradicionales de territorialidad, legalidad y de culpabilidad.[2]

A lo largo de las últimas décadas, este término ha sido analizado a la luz de diversos enfoques teóricos y disciplinarios, especialmente desde el derecho penal, las ciencias informáticas, y en menor medida por las relaciones internacionales, áreas que se han centrado en aspectos normativos y legislativos para enfrentar o al menos mitigar los delitos cometidos en el ciberespacio. Sin embargo, no se ha tomado en cuenta un campo multidisciplinario que permita desarrollar un esfuerzo académico conjunto para el desarrollo de políticas públicas en ciberseguridad y que contribuyan a la comprensión de la particularidad del cibercrimen. Por ello, en esta primera parte se realiza un análisis de los conceptos de cibercrimen y delito informático, términos que han sido usados popularmente como sinónimos sin distinguir su definición y procedencia.

Desde el punto de vista histórico - informático, la terminología del delito fue adaptándose al desarrollo de los equipos tecnológicos como de sus sistemas operativos, los entornos virtuales y a los cambios de patrones sociales que determinaron nuevas y avanzadas formas de infracciones cometidas en el ciberespacio. Así, en el año de 1970 se introdujo el término delito informático, y fue acuñado por primera vez por el académico

[2] Estos tres términos son especialmente discutidos desde el área del Derecho Penal, pero en este trabajo, se tratará de incluir dentro de los desafíos globales del cibercrimen y sus esfuerzos de implementación de medidas de ciberseguridad. Al final de este capítulo se profundizan sus aspectos legales necesarios para dar paso al análisis de las legislaciones latinoamericanas.

D.B. Parker (1976, citada en Holt y Bossler 2016) para referirse al mal uso de las computadoras. Se entendía por mal uso a toda actividad maliciosa dentro de los límites informáticos que ponga en riesgo la integridad física de la computadora. Cabe resaltar, que en este contexto, el acceso a equipos informáticos era limitado y su uso era especialmente corporativo o institucional. Por tanto, solamente un individuo que tenía conocimiento especializado sobre la computadora podía cometer tal delito.

Su concepto aún era limitado, sin embargo dadas los grandes avances tecnológicos y las nuevas intromisiones en los sistemas operativos por parte de usuarios para diferentes propósitos, para el año de 1998 se empezó a usar el concepto de cibercrimen para referirse a los delitos cometidos en la red. Aquí el perpetrador utiliza ya un "conocimiento especial en el ciberespacio" (Wall 2001, 2).

Según la reflexión de David Wall, las referencias conceptuales del cibercrimen, originalmente forma parte de la literatura del ciberpunk de las décadas de 1970 y 1980, época en que autores y directores de cine de ciencia ficción empezaron a relacionar y crear historias entre elementos tecnológicos y del ciberespacio con los movimientos punks. De esta narrativa, Wall observa que los orígenes de los conceptos de cibercrimen y ciberespacio tienen elementos "dramáticos, futuristas y distópicos",[3] debido a la carga ficcional que lleva consigo el uso de la tecnología.

El hecho notorio del concepto de cibercrimen es su asociación con el ciberespacio, poniendo en evidencia un nuevo término que discute el espacio-territorio, la temporalidad, el anonimato y las características de la realidad virtual. El delito como tal empieza a dar un giro hacia la complejidad de la tecnología y las conductas del ser humano en ambientes virtuales.

Esta apreciación permitió que académicos e investigadores puedan adoptar el concepto de cibercrimen como término que se refiere no solo a la manipulación tecnológica sino a la introducción y manejo de conocimientos sobre el ciberespacio. Sin embargo, en la visión jurídica (como en la mayoría de legislaciones) se sigue utilizando el término de

[3] Wall analiza los mitos y creencias (superhackers, impunidad, anonimato). que se han desarrollado alrededor del cibercrimen por la influencia de los medios de comunicación y de la ciencia ficción en la percepción del público sobre los hackers, ciberdelincuentes Distorsiones que han sido llevadas a la realidad y a la percepción del público sobre la ciberdelincuencia, generando un estado de shock o a una cultura de miedo (cyberfear-Wall 2007) o en palabras de Baudrillard al estado de vértigo de la realidad (vertige de la realité-1998).

delito informático, pero haciendo una distinción entre dos tipos de conductas: a) las que utilizan las herramientas informáticas en la acción delictiva y b) las que atacan o vulneran los bienes informáticos y sus componentes, cobijados por la protección jurídica del país (Páez 2010, 153).

Según este último, la definición de delito informático dependería del alcance de la legislación interna que tipifique aquellas infracciones, como también del avance del tratamiento jurídico a las conductas que utilicen estas herramientas para violar cualquier tipo de derecho. Los delitos pueden ser de distinta índole desde el robo de datos, manipulación, extorsión, fraude hasta daño o intromisión a sistemas.

Aunque aquí el término, sigue siendo el tradicional, se incluye de forma connotativa el significado de cibercrimen, lo que permitiría que las legislaciones puedan desarrollar y aplicar a su propio cuerpo normativo. Sin embargo, es pertinente que cada legislación o cuerpo académico identifique el alcance de los términos para no caer en contradicciones.

1.1 Tipología

La categorización del delito informático ha sido utilizada en el derecho penal y en las ciencias informáticas para desarrollar distintos tipos de respuestas. Desde el derecho penal se regulariza el espacio virtual a través de una legislación interna, mientras que desde las ciencias informáticas se crean programas y software para combatir las amenazas cibernéticas. Lo mismo sucede con un enfoque académico, cuyas categorizaciones se derivan de ambas experiencias para clasificar los cibercrímenes en diferentes grupos.

En recientes investigaciones (Turrini y Ghosh 2010) se ha tratado de sistematizar en dos grandes grupos para tener una visión clara de su tipología tanto en cibercrímenes técnicos y no técnicos. Los cibercrímenes técnicos se referirían a aquellos que se infringen mediante el uso de conocimientos técnicos y que no podrían causar "mayor daño".[4] Sin embargo, sigue siendo adverso y un factor potencial para ocasionar distintas amenazas. En esta categoría se incluye la piratería informática, los delitos maliciosos, los delitos contra la propiedad intelectual y la denegación de servicio. En cambio, los cibercrímenes no técnicos

[4] Este tipo de cibercrímenes son cometidos cuando el infractor ha logrado eliminar y extender alguna forma de control no autorizado sobre el sistema informático.

no requerirían mayor conocimiento y están relacionados con el ciberacoso y a las limitadas formas de violación de derechos de autor.

Esta clasificación profundiza en el concepto del ciberespacio, y va un poco más allá de la categorización tradicional del derecho penal, vincula los aspectos tecnológicos y los conocimientos que el individuo tenga sobre ellos para vulnerar la información, los datos, los equipos y todo lo relacionado con la realidad virtual. Sin embargo, sigue siendo limitada como punto de referencia para clasificar los distintos tipos de delitos que se modifican y transforman en nuevas modalidades en el ciberespacio. Por ello, se ha adoptado el aporte de Wall (2001) como propuesta mayormente aceptada y referenciada por diferentes académicos (Viano, 2017; Holt y Bossler, 2016; Koops, 2016), que agrupa delitos, desviaciones y toda actividad criminal relacionada con el ciberespacio en cuatro categorías: *cyber-tresspass* o intrusión, *cyber*-robo, ciberpornografía y ciberviolencia.

Cyber-trespass o intrusión

Se refieren a los ataques maliciosos y al acceso a cuentas de correo electrónico, así como a sistemas de información que no sean de su propiedad. Es una actividad asociada comúnmente con los hackers informáticos, quienes también pueden atacar estos sistemas con virus o algún tipo de *malware* (programas maliciosos).

Según la Contraloría General de Estados Unidos (*Government Accountability Office*, GAO), se estiman pérdidas de 100.000 millones de dólares anuales por piratería informática en el país norteamericano (Holt y Bossler 2016, 11). A simple vista esta cifra representa pérdidas millonarias para el sector informático, sin embargo, pone en evidencia la vulnerabilidad de los sistemas de ciberseguridad y de las propias políticas estatales que aún no pueden controlar totalmente el ciberespacio. Este aspecto está presente en todos los tipos de delitos y actividades criminales que se realizan en la realidad virtual.

Cyber-robo

Este grupo contiene todo lo relacionado con el robo de información, datos personales, públicos y financieros. Se puede incluir el ciberespionaje, (Mehan 2014) que implica el robo de información confidencial o secreta, relacionado a un Estado o a instituciones privadas. Para el caso de la agresión al Estado, los daños pueden ser

innumerables, especialmente por el manejo de datos públicos o relacionados con la ciudadanía. [5] Se convierte en un problema latente para toda la población, evidenciando la fragilidad de la capacidad estatal en la protección de información sumamente sensible con consecuencias severas para sus ciudadanos en la exposición a futuros cibercrímenes como el phishing o suplantación de identidad, estafas, robos de tarjetas de crédito, entre otros.

En el aspecto financiero son los delitos referentes a la clonación o las cookies de sitios web que roban números de tarjetas de crédito. En este espacio, se ha abierto un mercado de compra y venta de información financiera. Incluyen los robos cometidos a través de correos spam o encuestas en línea con información falsa para recaudar fondos o donaciones por internet. [6]

Ciberpornografía y obscenidades

Representa toda forma o contenido sexual y pornográfico que se pueda identificar, publicar, consumir y distribuir a través del ciberespacio. Algunos actos y materiales sexuales explícitos pueden ser legales o no, dependiendo de la legislación local. Debido al elemento anonimato en las redes, muchos delitos sexuales son inmunes a una debida sanción.

El ciberespacio puede ser entendido como un medio o soporte de reproducción y difusión de material pornográfico. Sin embargo, aquí la gravedad es más alta debido a que se pueden cometer diferentes delitos sin ser rastreados, también da cabida a otros formas de vulnerar los derechos humanos, sin que ello tampoco suponga una infracción ante la ley. En muchos países estas conductas no son entendidas como delitos.

Ciberviolencia

En esta categoría incluyen todo tipo de conductas que permita crear, distribuir o solicitar acceso a otros materiales que pueden ser dañinos y peligrosos para los usuarios. Se

[5] Por ejemplo en Ecuador, investigadores de la empresa vpnMentor, descubrieron en septiembre de 2019 información personal de 17 millones de ecuatorianos, en una base de datos en Miami accesible a todo público. Este hecho aún sigue en investigación por parte de la Fiscalía General del Estado (El Comercio 2019).

[6] Inclusive existen chats o foros como por ejemplo del Internet Relay Chat (IRCi, donde usuarios se comunican tanto en ruso como en inglés para obtener este tipo de información.

refiere específicamente al impacto psicológico o emocional que pueda causar a otros por la información o contenido que resulte perjudicial para la víctima.

Se refiere a la información que puede influir en el comportamiento de las personas como por ejemplo, la existencia de materiales en la web como guías y manuales de construcción de bombas o cualquier otra información que incite a la violencia. En este punto se podría hablar de una nueva modalidad de aprovechar los recursos del internet por diferentes grupos criminales que utilizan este espacio para difundir información acerca de sus organizaciones y subir contenido (manuales de bombas, armas) que de alguna forma los relacione y vincule con ellos. Aunque esto no esté totalmente comprobado, el ciberespacio es una plataforma que almacena cuanta información exista y la creatividad humana se ingenie para cometer cualquier tipo de delito que aún no haya sido identificado o tipificado. Por tanto, la ciberviolencia es un tipo de cibercrimen que alberga otros tipos de delitos que fácilmente puede pasar por desapercibidos y transformarse en otras formas de conductas adversas.

Se debe resaltar que estos cuatro grupos no solo incluyen el término *cyber* como un elemento diferenciador, trasponiendo las mismas conductas y acciones que suceden en el mundo real. El ciberespacio transforma el concepto tradicional del delito y permite el desarrollo de nuevas conductas y comportamientos humanos que difieren del mundo físico. Transforma a los individuos en avatares que juegan con las reglas del tiempo, el espacio, los códigos sociales y la norma, consintiendo la realización de una infinidad de acciones y encuentros entre lo permitido y lo no permitido. La especialidad del cibercrimen es la sombra que encubre los propósitos de los delitos y la insospechada razón detrás de cada acción.

Las ciencias informáticas y el derecho penal se encuentran siguiendo estelas de estas sombras, en el que muchas de las veces, solo logran identificar a sus peones y no a los verdaderos actores intelectuales que son parte de grandes organizaciones criminales. Pese a ello, estas dos perspectivas han logrado identificar y presentar una clasificación aproximada al ciberespacio. En el campo de las relaciones internacionales, el cibercrimen se ha podido vincular y contextualizar en dos grandes modalidades como delitos internacionales y delitos transnacionales, que a continuación se analiza dentro de la problemática de las redes criminales.

1.2 Delito internacional versus delito transnacional

El desarrollo del ciberespacio ha fortalecido las redes criminales y las formas de cometer delitos sin ser identificados, además porque la mayoría de países no cuentan con una amplia tipificación del cibercrimen ni un proceso investigativo adecuado que pueda rastrearlos. Muchos de estos delitos pueden ser cometidos por grupos delictivos así como por personas o hackers que fungen en el anonimato para satisfacer sus propias necesidades y cumplir diferentes objetivos (políticos, económicos, sociales, ideológicos).

Teniendo en cuenta el contexto de la globalización y del surgimiento de nuevos actores no estatales en la economía mundial y en las dinámicas de la sociedad, el tradicional concepto del Estado se ha visto modificado, llegando incluso a ceder sus capacidades de regulación y organización a empresas multinacionales, transnacionales y organismos financieros (Zúñiga 2016, 64). Esta particularidad es aún más evidente en el ciberespacio, donde el esquema de Estado-territorio pierde sus fronteras, y hace posible que diversos actores no estatales vulneren las legislaciones y puedan cometer distintos actos delictivos.

Las posibilidades que abre el ciberespacio son infinitas y ofrece a los usuarios una multiplicidad de opciones para cometer delitos ya sea de forma individual o grupal. Similar a las estructuras organizadas pueden formar parte de una red que opere en diferentes Estados o solamente trabajar de forma aislada por interés propio y causar diferentes formas de daños tanto a la infraestructura del internet como a la sociedad misma (Holt y Bossler, 2016).

En este ámbito, existen tres términos que suelen ser confundidos entre delitos graves, grupos delictivos organizados (organización criminal) y crimen transnacional. Así para el cibercrimen puede ser entendido como un delito grave o dependiendo de su alcance como un delito transnacional o una organización delictiva con proyecciones internacionales. Para tener más claro se tienen las siguientes dimensiones que ayudarán a comprender su alcance (Zúniga 2016, 110):

- Delito internacional. Son los delitos que atraviesan diferentes culturas, nacionalidades o territorios.[7] Este tipo de delitos violan solamente el derecho

[7] Para el caso del virus denominado *Love Bug*, conocido como uno de los grandes cibercrímenes internacionales, que causó grandes daños y pérdidas millonarias a nivel mundial durante el año 2000, fue debatido por diferentes investigadores criminales y organizaciones internacionales (Goodman 2010; Bajovic, 2017) Este virus fue creado en Filipinas, afectando a más de 45 millones de usuarios en 20 países que fueron

internacional, es decir a los bienes jurídicos supranacionales, donde se busca una "responsabilidad individual internacional directa" (Zúñiga 2016, 78).

Bajo esta categoría se pueden incluir aquellos delitos contra el delito internacional como el genocidio, crímenes de guerra, delitos de lesa humanidad o las violaciones a los derechos humanos contra niños, niñas y mujeres. Son aquellos que lesionan o vulneran los derechos de la comunidad internacional.

- Delito transnacional. A diferencia del primer término, éste se encuentra relacionado con las estructuras del crimen transnacional organizado, y es utilizado como un concepto jurídico. En el orden práctico viola tanto el derecho interno, o su legislación doméstica, y el derecho internacional. Busca una responsabilidad, en el ámbito de organizaciones sujetos a las propias medidas implementadas por los Estados. Según la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, cada Estado parte adoptará medidas apropiadas conforme a su derecho interno.[8] Estos delitos lesionan tanto su jurisdicción interna (si se encuentra tipificado) como al derecho internacional para desarrollarse en un fenómeno global que involucra la participación de organizaciones delictivas. Por ejemplo la piratería, el tráfico de armas, el narcotráfico, trata de personas, el terrorismo, entre otros.

  Los conceptos de delitos internacionales y transnacionales están determinados por su tratamiento dentro de cada legislación ya sea ésta de orden nacional o internacional. En otras palabras, si se incluye el concepto de organización o estructuras delictivas en el derecho internacional, no significa que éste pueda ser

---

víctimas de pérdidas de información, destrucción de documentos y robos de contraseñas, con enormes consecuencias económicas.

Entre los afectados se encontraron empresas, bancos, hogares e inclusive servidores de agencias estatales. Los daños fueron diversos desde la deshabilitación de cajeros automáticos en Bélgica, baja de servidores de correos electrónicos como de L´Oreal en Francia, inhabilitación del 70% de computadores en Alemania, Noruega y Suiza, e incluso Microsoft fue afectado en las ciudades de Washington y Redmond en Estados Unidos (Goodman 2010).

A pesar que lograron rastrear al sospechoso, un ex estudiante de informática, por colaboración de agentes y expertos informáticos estadounidenses, éste no pudo ser sentenciado. En ese momento, las leyes de Filipinas no contaban con una tipificación del cibercrimen o delitos como el fraude, o distribución de virus que pudiera ayudar a una mayor investigación sobre los posibles actores ocultos en el anonimato y que posiblemente formarían parte de alguna red criminal cibernética o al menos estar relacionada con alguna otra organización (Goodman 2010).

[8] ONU Asamblea General. Convención de las Naciones Unidas contra la delincuencia organizada transnacional y sus protocolos. 15 de noviembre de 2000. Resolución 55/25

parte de su legislación nacional y que se tipifique como delito transnacional. Su aplicación varía según el grado de comprensión del delito internacional o transnacional en cada legislación interna.

- Crimen transnacional organizado. Son aquellos que lesionan los bienes jurídicos comunes a varios Estados y opera bajo una estructura organizada. Viola tanto la normativa nacional como internacional haciendo más vulnerable la identificación de actores estatales, no estales o las organizaciones implicadas.

El cibercrimen puede transformarse en cualquiera de las tres dimensiones mencionadas. Es decir, puede tener un alcance internacional si vulnera el derecho internacional, o transnacional si se convierte en una amenaza interna como externa dentro de los límites de su derecho interno y del derecho penal internacional. Pero qué sucede si éste proviene de una organización criminal organizada. ¿Puede entenderse en la forma tradicional de criminalidad organizada transnacional? ¿Cumple con los mismos propósitos? El crimen transnacional dentro de una estructura organizada opera de diferente manera, ya que no solo lesiona el derecho internacional, lesiona las jurisdicciones nacionales, siempre y cuando, éstas contemplen también los tipos de delitos y su tratamiento correspondiente en concordancia con la normativa internacional.

Para entender el funcionamiento de esta modalidad, investigadores y académicos concuerdan que es necesario comprender el concepto de redes sociales como sistemas estructurados que operan en diferentes niveles. Para el caso de la *cibercriminalidad organizada*, muchos de estos grupos son pequeños y poco estructurados (Neto 2017, 186). No siempre operan bajo la misma lógica de las redes tradicionales del crimen organizado y sus objetivos son distintos. En estas organizaciones las relaciones entre los ciberdelincuentes pueden ser transitorias o transaccionales.

El ciberespacio permite crear redes temporales para que estas actividades delictivas también puedan ser fluidas y mayormente flexibles ofreciendo la posibilidad de beneficiarse mutuamente sin la necesidad de formar una agrupación estructurada y permanente (Neto 2017). Por lo tanto, muchos de los grupos criminales transnacionales

hacen uso de este recurso sin requerir mayor conocimiento técnico para cometer delitos, solamente el servicio de un hacker para conseguir sus objetivos en el ciberespacio.[9]

A diferencia del crimen transnacional, no posee una jerarquía que funcione como una organización tradicional ya que puede operar en distintos países y sus colaboradores pueden tener distintos roles. Sin embargo, esta idea se ha ido modificando debido a la formación de pequeños grupos y subgrupos de hackers o ciberdelincuentes que han sabido aprovechar de sus conocimientos para formar redes criminales transnacionales y altamente interconectadas con una jerarquía estructurada.

A partir de esta jerarquía y organización relativas, se ha identificado que existen tres tipos de redes cibercriminales organizadas que operan en el ciberespacio (Choo y Grabosky 2013 en Neto 2017):

- Como nuevo camino. Las redes criminales tradicionales utilizan las TIC´S solamente como herramientas para mejorar sus actividades delictivas. Acceden al servicio de hackers o de la piratería informático para su beneficio propio.
- Como nueva forma. Son las organizaciones cibercriminales que se originaron y operan solamente en el ciberespacio. Sus miembros son individuos con conocimientos técnicos y especializados en operaciones cibernéticas. Son organizaciones más pequeñas y menos jerarquizadas que las tradicionales.
- Motivaciones ideológicas y políticas. Son organizaciones relacionadas con el ciberterrorismo y el hacktivismo que ofrecen a otras organizaciones o redes terroristas, servicios de inteligencia, encriptamiento, propaganda política, *cybergroomed* (reclutamiento).

Cualquiera que sea la modalidad, el cibercrimen sigue actualizándose a través de las redes criminales que se han especializado en el uso de la tecnología y del ciberespacio para fortalecerse. Del mismo modo, las nacientes redes cibercriminales pueden convertirse en poderosas agrupaciones transnacionales que aprovechen de sus conocimientos técnicos para ganar el mercado cibernético que es un nuevo espacio en pugna entre diferentes actores estatales y no estatales.[10]

[9] Investigaciones recientes han encontrado que las actuales mafias italianas, rusas, nigerianas y tríadas chinas, así como carteles colombianos y mexicanos, han desarrollado alianzas estratégicas y nuevas relaciones de negocios entre ellos a través del ciberespacio (Goodman 2010, 312).

[10] Este tema se analiza dentro de los desafíos globales del cibercrimen.

2. La corriente criminológica en el estudio del cibercrimen

Es importante revisar la corriente criminológica en el estudio del cibercrimen para comprender cómo se configuran las nuevas tendencias en su análisis teórico. Pues, desde los años setenta se empezó a discutir, no solamente los alcances del cibercrimen sino las conductas humanas en ambientes virtuales y la transformación del delito en el ciberespacio.

Los primeros estudios se basaron, especialmente los de Grabosky (2001), en los análisis de las teorías dominantes de la criminología tradicional como la teoría de las actividades rutinarias de Cohen y Felson (1979), arraigo social (Hirschi 1990), autocontrol y aprendizaje social (Bernard. 2010) y teorías de las subculturas (Miller 1958); trasladando el mismo cuerpo conceptual de víctima y delincuente a un ambiente cibernético. Sin embargo, dados los avances tecnológicos, académicos e investigadores, vieron la necesidad de desarrollar nuevas perspectivas teóricas que permitan comprender la relación entre lo virtual y la cibercriminalidad (Holt y Bossler 2016).

En el caso de las teorías de la elección racional y las actividades rutinarias aportaron con una nueva metodología para el estudio de diferentes crímenes denominado como Prevención del Crimen Situacional (PCS, Clake 1983, Cornish y Clarke 2003). Se basa en que el delincuente analiza los riesgos, los posibles beneficios y los factores sociales o situacionales antes de cometer el delito. Para comprender estas conductas y prevenir los delitos, los autores identificaron cinco categorías que pueden ayudar para influir en la toma de decisiones del delincuente: el desafío en la participación como factor riesgo para llevar a cabo dicha actividad; la reducción de las recompensas que pueden resultar del delito; la reducción de las provocaciones para ofender; y la eliminación de cualquier excusa que justifiquen el delito. [11]

Esta metodología permitió que en el campo informático diera paso al análisis geoespacial, donde examinaron la distribución espacial de violaciones de datos como técnica de prevención del delito (Khey y Sainato 2013, en Holt y Bossler 2016). Sin embargo, encontraron dificultades en ubicar un patrón en la violación de datos para identificar a los posibles autores. Lo que significaba que las organizaciones y los

[11] Estas características forman parte de los enfoques de prevención propuestos por Clarke, 1983, 1997, 1999; Cornish & Clarke, 2003, en Holt y Bossler 2016.

ciberdelincuentes poseían recursos y los conocimientos técnicos para burlar los sistemas de seguridad y encontrar formas de no dejar patrones o rastros en el ciberespacio.

Justamente las ciencias informáticas en conjunto con las teorías de prevención conjugaron novedosas metodologías que ayuden a construir patrones y algoritmos que identificaran los ciberdelitos. Sin embargo, esta lógica es superada por la propia tecnología que logra duplicar y saltar coordenadas difíciles de rastrear por estos programas informáticos. A partir de este desafío nace el estudio de la *criminología virtual-híbrida* que fue discutida desde mediados de los noventa para entender las nuevas realidades, conductas humanas y la psicología del delincuente en el espacio virtual y tecnológico (Brown 2013). Analiza el comportamiento humano y su relación con la tecnología, en una fusión entre lo humano y lo no humano (híbrido). Pues el límite que se explora es justamente la influencia de la tecnología en las relaciones humanas y por tanto en su comportamiento.

Más tarde, el académico Tim Owen (2017, 5)[12] retoma las ideas de Brown y propone una nueva perspectiva teórica denominada Genética Social y añade los meta-conceptos de *neuro-agencia*, las categorías de seres humanos (*dasein*)[13] y de *verdad óntica* de Heidegger (psicobiografía).[14] Aunque en este este estudio trata de asuntos gnoseológicos sobre la verdad y las condiciones psico-sociales. El autor propone que la criminología virtual-híbrida se convierte en un puente conceptual entre la cibernética, la realidad virtual, las teorías de la información y comunicación y la psicología (neurociencia) para entender la relación de medio ambiente (contexto socio cultural), máquina (tecnología) y ser humano.

De ahí que las nuevas teorías en el estudio del cibercrimen se hayan volcado sobre las redes de relaciones de los seres humanos y el medio ambiente, debido no solo a la existencia de categorías psico-sociales, sino por la complejidad del ciberespacio que alberga otras formas de comprensión y de conductas humanas.

---

[12] El autor profundiza en los elementos causantes del mundo exterior y cómo estos influyen de manera física y biológica de los individuos, determinando cierto comportamiento o reacción. Factores que pueden predisponer cierto comportamiento pero el individuo está en la capacidad de tomar una decisión (neuro-agencia).

[13] El primer término neuro-agencia se refiere a la condición genética humana producto de una evolución natural pero diferenciada del resto por su capacidad de libre albedrío. En cambio, el segundo término se refiere a los aspectos únicos y asociales heredados dentro de un contexto social, político y económico (elementos causales del comportamiento humano). Por tanto conjugados estos dos términos, revelan la complejidad de la relación máquina-ser humano.

[14] Análisis de las características psicosociales de los individuos.

2.1 Nuevas teorías en el estudio del cibercrimen

Arriba se mencionó cómo la criminología se inscribe hacia un nuevo campo de estudio que permita, no solo trasladar los conceptos tradicionales de la criminología, sino en abrir un puente teórico con otros estudios como la informática, la biotecnología, la neurociencia, las teorías de la comunicación, entre otros. En este sentido, Thomas Holt y Adam Bossler (2016) desarrollan una exposición teórica sobre el ciberdelito desde diferentes investigaciones, entre ellas criminológicas, combinando sus diferentes corrientes para comprender cómo su concepto se ha ido desarrollado en conjunto con las tecnologías de la información y la comunicación, convirtiéndose en una amenaza mundial, tanto para los individuos como para las instituciones estatales.

Estos autores proponen estudiar el cibercrimen desde diferentes corrientes que ayuden a comprenderlo y por tanto a buscar nuevas formas de lucha contra éste donde exista la necesidad de mejorar las investigaciones sobre delitos informáticos a través de la colaboración entre académicos y profesionales de diferentes ramas como la informática, psicología, ciencias políticas, entre otros. Estos estudios están relacionados con la criminología con modelos propios de análisis del ciberespacio como: la teoría de Deriva Digital, la teoría de la transición espacial y la teoría de red de actores.

Teoría de la Deriva Digital

Presenta el concepto de *digital drift* o deriva digital de Goldsmith y Brewer (basados en la teoría de la Deriva de Matza 1964). Esta teoría propone un modelo integral que analiza cómo la tecnología y el uso de internet, permiten a los usuarios jugar con elementos de la asincronisidad y el anonimato, es decir, la ausencia de regulación y de normas, producen comportamientos diferentes y desinhibidos poco habituales a la realidad.

Bajo estas características se producen dos condiciones en el ciberespacio que favorecen la deriva de los individuos: la afinidad y la afiliación. El uno es la capacidad de sentirse identificado y el otro el sentido de pertenencia a un grupo determinado en el que pueden profundizarse su desviación y sus habilidades. Por ejemplo, asociaciones con otros grupos afines como piratería digital, chats privados, actividades que pueden presentarse como espacios atractivos a diferentes individuos (Holt y Bossler 2016, 90).

Teoría de transición espacial

Esta teoría proviene de la propuesta teórica de K. Jaishankar (2008), basado en el comportamiento de las personas dentro y fuera del internet, argumentando que son distintos roles que asume el individuo. Se sostiene en siete proposiciones que entre las principales están: a) las personas que reprimen su comportamiento en el mundo físico tienen más probabilidades a cometer estas acciones en el ciberespacio; b) mayor probabilidad a que los delitos en el ciberespacio se cometan también en el mundo físico y viceversa; y c) las sociedades cerradas pueden producir mayores niveles de ciberdelincuencia que las sociedades abiertas debido a la naturaleza represiva de los regímenes gubernamentales (citado en Holt y Bossler 2016).

Algunas proposiciones aún no han sido comprobadas teórica o empíricamente por otros académicos que den cuenta de su lógica. Es un acercamiento que permite entender algunas variables de la ciberdelincuencia como el anonimato y la propensión de los delitos que son comunes en el mundo físico y otros en el mundo virtual. Del mismo modo, otras proposiciones aún son difíciles de comprobar como por ejemplo la afirmación de que los individuos que cometen algunas formas de delito cibernético como el acoso o *ciberbullying* también son los mismos individuos que cometen crímenes tradicionales en el mundo físico. Muchas de estas afirmaciones no son universales y están sujetas a diferentes contextos sociales, políticos y económicos que no siempre revelan un mismo patrón o la misma lógica de operación que en el mundo físico.

Teoría de red de actores

Supone el conjunto de redes entre máquinas, robots, computadores que operan a través de otros sistemas operativos (red de *bots*) para manipular, distribuir e infectar a diferentes redes que permitan cometer un sin número de delitos en el ciberespacio. Se basa en un enfoque construccionista social en el que la tecnología tiene un papel central en diferentes acciones, dando lugar a los *bots* como híbridos criminales que resultan de la interacción entre humanos y la tecnología misma (Van der Wagen y Pieters 2015).

Para estos autores, más que una teoría se trata de un enfoque sensibilizador, que permite entender esta relación como parte de un todo, y a examinar a la tecnología como un

elemento que puede prescindir de la mano humana, ya que ésta maneja otras redes por sí sola, algo que los seres humanos no pueden.

En conjunto estas teorías presentan nuevos escenarios que modifican la manera de comprender el cibcercrimen. Primero está las condiciones de deriva o de afiliación para formar parte de entornos virtuales (elementos de afinidad y afiliación); segundo, los roles o configuración de avatares (ciberdelincuente) que difieren del mundo real y crean nuevos mundos virtuales sujetos a distingas reglas de juego, y tercero, la presencia de *bots*, un elemento riesgosamente autónomo que puede prescindir del ser humano, después que se lo haya configurado para un determinado objetivo.

3. Desafíos globales del cibercrimen resultantes del uso de los medios informáticos

Los diferentes cuerpos teóricos y la literatura al respecto del cibercrimen no solo se han preocupado por su definición sino también por las nuevas y crecientes formas de delitos que se pueden cometer en el ciberespacio bajo las figuras del anonimato y la fragilidad de los sistemas de seguridad y de las legislaciones (locales e internacionales). A esto se suman los nuevos avances tecnológicos y el desarrollo de redes criminales que se dotan de mejores herramientas tecnológicas (*bots*), para satisfacer diferentes intereses personales, políticos, ideológicos, sociales o económicos.

Uno de los grandes errores en la identificación de estos desafíos es el planteamiento de un enfoque clasificatorio que solo enumera los efectos negativos del cibercrimen y no su relación con los intereses o propósitos que cumplen los distintos cibercrímenes. Es decir, se ha trazado solo una línea entre los desafíos resultantes y sus efectos generalizadores. Para lo cual esta investigación, luego de enumerar y revisar cada desafío, se optó por agruparlos en dos grandes actores: el Estado y el mercado (sector empresarial corporaciones, empresas, instituciones privadas); cuyas acciones y formas de respuesta también son distintas frente a cada situación.

3.1 Desafíos para el mercado

Las preocupaciones que nacen de estos desafíos son las consecuencias sobre los aspectos económicos y financieros que pueden producir efectos negativos sobre la integridad de las empresas y corporaciones. Entre los factores desafiantes se encuentran: los

tipos de usuarios, los tipos de amenazas o cibercrímenes; y el funcionamiento de mercado clandestino o economía paralela a la real (legítimamente constituida).

3.1.1 Tipos de usuarios

El mercado se encuentra conformado por instituciones privadas y empresas que forman parte del sector empresarial que difiriendo de su actividad comercial, cuentan con sus propias unidades informáticas que brindan soporte a sus propias instituciones (manejan complejos sistemas informáticos y bases de datos gigantescos) o reciben la asesoría de empresas privadas en ciberseguridad. El otro tipo de usuario es el público general o el pequeño usuario del internet que maneja redes domésticas y privadas para uso personal.

El sector empresarial, pese a encontrarse asesorado por empresas en ciberseguridad también es vulnerable a ataques cibernéticos. En cambio, el usuario común es el más proclive a ataques informáticos y a entregar más fácilmente información personal debido al poco conocimiento y manejo de sistemas de protección de datos. Para Koops (2016) este panorama forma parte de un desafío al que denomina la megatendencia de la erosión de la privacidad, donde los usuarios comunes son más vulnerables a posibles ataques informáticos. El internet se configura como el espacio en el que todo puede pasar y más si no existen las garantías de seguridad y privacidad en el manejo de sus equipos informáticos, ya sean estos usuarios comunes o corporativos, todos somos posibles víctimas de algún tipo de cibercrimen.

3.1.2 Tipos de amenazas

El nivel de victimización del crimen cibernético es mucho más alto mientras que el nivel de sus denuncias es mucho menor en comparación con la criminalidad tradicional (Bajovic; Viano 2017); los daños y las cuantiosas pérdidas económicas siguen creciendo, mientras las medidas de ciberseguridad aún siguen siendo vulnerables.

Las amenazas o cibercrímenes dirigidos a este sector tienen como propósito robar datos o vulnerar sistemas con fines comerciales. Por tanto, los ciberdelitos utilizados pueden variar desde el *phishing*, *ransonware* hasta robo de investigaciones o informaciones secretas (fórmulas o procesos científicos), desvío de información reservada pertenecientes a grupos económicos, es decir, información sensible que puede servir a otra para la creación

o formulación de productos y/o servicios. En este grupo también se incluyen todos los delitos relacionados a la violación de los derechos de propiedad intelectual para el lucro de otros grupos o individuos.

En 2017 la compañía internacional de seguridad informática, Kapersky realizó un estudio estadístico en el que se encontró que en Latinoamérica existe un ataque informático cada 12 segundos. Además especificó que el delito mayormente cometido es el *ramsonware,* secuestro de datos e información a cambio de dinero.[15] El *ransonware* o secuestro de datos se configura como otras de las modalidades del cibercrimen que genera un negocio millonario para los ciberdelincuentes. Consiste en infectar mail y documentos mediante un sistema denominado CryptoLocker, mecanismo que permite a los individuos solicitar dinero para recuperar sus documentos. Los precios para recuperarlos pueden oscilar entre 300 y 1000 dólares (Mehan 2014). Un ejemplo de ello, sucedió en 2016 donde una empresa fue infectada con este *ransonware* cada 40 segundos. Según Cybersecurity Ventures estima que para el 2019 se puede incrementar a cada 14 segundos y para el 2021 a cada 11 segundos.[16]

3.1.3 Mercado clandestino

En este espacio se dinamiza la economía clandestina del cibercrimen, uno de los grandes desafíos, [17] incluso más complejos que otros mercados como el narcotráfico (Koops 2016), en el que las autoridades y las legislaciones están limitadas por las redes complejas que se tejen entre ciberdelincuentes y organizaciones criminales.

---

[15] Dinero, 2017. El apetitoso negocio del cibercrimen. Se pude revisar en: https://www.dinero.com/edicion-impresa/tecnologia/articulo/las-cifras-que-mueven-el-cibercrimen-a-nivel-global/241593

[16] El Instituto de Investigaciones Ponemon (dedicada al desarrollo de investigaciones independientes sobre la protección de datos y las nuevas tecnologías de la información) determinó que Estados Unidos, es el país que invierte más en estudios del cibercrimen en comparación con otros países de la región. En 2013 han invertido alrededor de $ 11,56 millones de dólares por organización, Alemania $ 7,56 millones, Japón $ 6,73 millones, Reino Unido 4,72 millones (Mehan 2014).

[17] Las formas de pago que se realizan en este mercado han dado lugar también a las transacciones en criptomonedas o bitcoins. Método que facilita el anonimato de las partes sin la intervención de los sistemas de las instituciones financieras. El acceso al mercado negro o al criptomercado se lo realiza mediante el navegador Tor , que da lugar a un millón de transacciones por un valor estimado de 1.200 millones de dólares en ingresos. Este incremento se dio especialmente por las transacciones hechas por la denominada Ruta de la Seda , una red creada en 2011, un sitio web para la adquisición de diferentes materiales desde ropa, equipos tecnológicos hasta drogas (Holt y Bossler 2016).

El ciberespacio permite la formación de un mercado negro donde ofertan un sin número de productos tecnológicos como *bots* y sistemas informáticos para el hackeo o robo de información de diferentes empresas. Aquí tanto redes criminales como ciberdelincuentes pueden acceder de forma clandestina a estos servicios que se comercializan en el internet (Mehan 2014, Viano 2017). Este espacio se le conoce comúnmente como *deep web* o *dark web*, que funciona mediante otros exploradores de internet alternos a los tradicionales, en donde se puede encontrar una variedad de información, especialmente clandestina e ilegal. Sirve para el comercio de bienes y servicios y el establecimiento de otras redes criminales que se comunican y fortalecen sus relaciones delictivas mediante chats privados e información encriptada. Permite la formación de foros dedicados a tráfico de drogas, números de tarjetas de crédito, material o contenido ilegal que puede violar los derechos humanos (Neto 2017).

Un desafío que se relaciona con este mercado son las tecnologías de ocultamiento de información (esteganografía),[18] operaciones e identidad que utilizan los individuos para dificultar su rastreo. Una estrategia que puede ser útil tanto para ciberdelincuentes como para activistas sociales y políticos que ocultan su identidad.

Bajo estas condiciones, uno de los posibles desafíos por el desarrollo de las tecnologías y las ventajas del anonimato es el incremento del crimen organizado, quienes utilizan el internet y las herramientas tecnológicas para crear y mejorar redes criminales y ejecutar sus actividades a nivel mundial.

3.2 Desafíos para el Estado

Para el Estado los desafíos globales del cibercrimen difieren del mercado no solo por sus fines, sino por su alcance estructural. Aquí estamos hablando de los alcances sociales, políticos y económicos que pueden poner en riesgos las infraestructuras críticas.

3.2.1 Tipos de actores

A diferencia de los actores del mercado, el Estado viene a ser la estructura orgánica conformada por instituciones públicas y privadas que ofrecen sus productos y servicios para

[18] Ocultamiento de textos o documentos dentro de una imagen, audio o video. En 2011, un caso similar fue encontrado en Berlín dentro de una tarjeta de memoria con un video pornográfico, en el que se identificó 141 documentos relacionados con operaciones del grupo Al Qaeda (Mehan 2014).

la atención integral del ciudadano. Por ello, al hablar de actores, son los relacionados con las instituciones, y estos pueden ser internos o externos.

Para el Estado uno de los grandes desafíos es la identificación de amenazas provenientes de este tipo de actores. En el primer caso, son los individuos que forman parte de la institución, tienen acceso autorizado y legítimo a las redes, computadoras e información, que les permiten vulnerar más fácilmente los sistemas de seguridad. Son amenazas altamente peligrosas para las instituciones puesto que conocen el funcionamiento de sus sistemas y saben cómo esquivar las medidas de ciberseguridad implementadas en sus propias instituciones.

El segundo tipo de actor, en cambio, no tiene ningún tipo de relación con la institución atacada y opera fuera de la red. Puede ser cualquier individuo u organización con diferentes intereses políticos o sociales para poner en riesgo las infraestructuras críticas que maneje aquella institución. Cabe recalcar, que durante los años ochenta y noventa los ataques externos eran mínimos, mientras que los ataques internos iban en incremento justamente por su facilidad de acceso a las redes compartidas en las instituciones. Sin embargo, desde mediados de los noventas los ataques internos fueron disminuyendo, y los externos llegaron a ser más comunes (Holt y Bossler 2016).

Entre las motivaciones para los ataques internos como externos pueden ser varios. En el caso de los actores internos estos tienen la oportunidad de aprovechar de sus recursos y su accesibilidad en beneficio propio. La de los externos, es mucho más amplia ya que pueden ser motivaciones políticas (datos públicos), financieras (tarjetas de crédito, *phishing*), sociales o entretenimiento.

3.2.2 Tipos de amenazas

La preocupación por parte del Estado se centra principalmente en la variedad de cibercrímenes utilizados para cumplir distintos intereses políticos-ideológicos y sociales, como: la falsificación de datos, la modificación de sistemas y la afectación a infraestructuras críticas. En cuanto a los objetivos políticos se identifica la intromisión en los sistemas de datos para la modificación o alteración de los sistemas de votación para causar pánico en tiempos de elecciones cuando el voto es electrónico o la falsificación de

datos cuando se procesa la información. Es decir, mientras mayor sea el componente informático en el procesamiento de datos mayor será el riesgo de ser vulnerado.

Este hecho ha sido relacionado con la aparición de nuevas tendencias como el ciberterrorismo, *cybergrooming* y ciberguerra. Fenómenos sociales y políticos sumamente complejos que se debaten entre académicos provenientes de diferentes escuelas, especialmente, norteamericanas (Mehan 2014, Noble y Edwards 2017).

Ciberterrorismo

En primer lugar, el terrorismo se definió como una actividad criminal para difundir miedo a través de la destrucción, violencia o muerte. Sin embargo, es a partir del 11 de septiembre de 2001 que el sistema internacional se modificó y trajo consigo nuevos actores no estatales en los escenarios políticos, económicos e ideológicos. Estos actores han podido fortalecerse a través del uso de tecnologías y sistemas informáticos para realizar ataques cibernéticos y dañar gravemente las infraestructuras esenciales en el funcionamiento de servicios básicos como redes eléctricas, interrupción de servicios bancarios, sistemas de transporte aéreos y robo de datos reservados o secretos. Pueden hacer uso de las tecnologías de la computación como armas u objetivos que son destinados a afectar a un Estado y por tanto generar miedo en sus ciudadanos. Sus propósitos son esencialmente ideológicos, religiosos y políticos (Mehan 2014, Neto 2017).

En una investigación realizada en 1999 por el Centro de Estudios del Terrorismo y la Guerra Irregular de California (Mehan 2014), determinó que existen tres niveles de grupos terroristas que ejecutan sus ataques en el ciberespacio: estructuras simples no estructuradas, avanzadas y complejas coordinadas, cada una con distintas capacidades para cometer actos terroristas. Estos tres niveles reflejan cómo se implementan estrategias de vulneración de redes y sistemas de información mediante el conocimiento técnico y dominio del ciberespacio.

Cybergroomed

En virtud de lo expuesto, el internet se ha convertido en un espacio mayormente utilizado por organizaciones terroristas para comunicarse y desarrollar sus actividades delictivas, sin embargo, ha surgido una nueva modalidad de reclutamiento que las

organizaciones aprovechan para disuadir a cualquier tipo de usuario. Esto se conoce como *cybergroomed*, donde, particularmente, mujeres jóvenes son reclutadas.[19] En las investigaciones de *Home Affairs Select Committee on Counter Terrorism* de Reino Unido, en 2016 se estimó que entre 700 y 800 personas viajaron del país británico a Siria para unirse a grupos extremos del Estado Islámico (*IS* por sus siglas en inglés), de las cuales 50 a 60 son mujeres adolescentes ciber-reclutadas (Edwards 2017, 32).

Ciberguerra

El internet genera un espacio de intromisión de diferentes actores y batallas, que difieren de la visión tradicional del mundo físico. Es un espacio donde se libra la guerra de la información, *Information warfare* (Noble 2017) o en palabras de Mehan (2014), una guerra cibernética o *cyberwarfare* en diferentes escalas.

Estos términos han sido utilizados como sinónimos aunque ambos tienen diferentes significados. El primero incluye las técnicas del cibercrimen como el robo de datos, ciberataques, uso de malware, espionaje, ciberterrorismo, entre otros. Según Mehan existen cuatro niveles o clases de ciberataques que se agrupan para medir el nivel de intensidad de conflictividad:

- Clase I o de baja intensidad. Son los ataques relacionados con información personal o privada.
- Clase II o en ascenso. Son los relacionados con el espionaje industrial y económico, contra una nación, empresas, universidades y otras estructuras organizacionales.
- Clase III. Se relaciona con el ciberterrorismo y todo ataque contra infraestructuras críticas (servicios básicos, redes eléctricas). Sus métodos se dirigen a Estados y gobiernos y su alcance es global.
- Clase IV. Se refiere a la guerra cibernética como máximo nivel de conflictividad que se libra en el espacio con objetivos mundiales.

[19] Algunos testimonios de mujeres explican que son matrimonios arreglados por la propia IS y que desconocían de estos arreglos; sin embargo, existen otros testimonios que afirman que sí conocían el propósito de su viaje para formar parte de estos grupos. También existen casos de mujeres que son utilizadas como esclavas sexuales (Jacoby 2015, citado en Edwards 2017). Un mercado que funciona dentro de estas agrupaciones donde se legitiman los discursos ideológicos apoyados en la fe musulmana y contra el colonialismo occidental.

La ciberguerra se refiere a la posibilidad futura de unir los cuatro niveles de la guerra informática en su conjunto, con el propósito de crear una guerra a nivel global, utilizando tácticas militares y tecnológicas con daños ilimitados. Sin embargo, para Mehan hablar de ciberguerra aún es una idea temprana, ya que ningún ataque cibernético cumple con los tres postulados de Clausewitz,[20] para determinarlo como un acto de guerra.

Justamente los tipos de ciberataques son confundidos con la ciberguerra por sus niveles de tensión que pueden existir en ambientes cibernéticos. Lo que puede causar también que se genere la idea de una posible ciberguerra es la influencia de los medios de comunicación sobre las tensiones existentes entre las grandes potencias y su relación con ciberataques.[21]

4. Esfuerzos de implementación de medidas de ciberseguridad

Siguiendo esta línea de análisis se han dividido en dos diferentes grupos, por cuanto las formas de respuesta del Estado y el mercado son distintos. Por un lado, los programas de seguridad cibernética y los millones de dólares invertidos por las empresas, y por otro, las políticas públicas de ciberseguridad implementadas por los Estados. Aunque en ambos, grupos, pueden combinarse estas medidas, los indicadores revelan que el sector empresarial tiene un objetivo lucrativo, mientras que los gobiernos se dirigen a la protección de las infraestructuras críticas y de los sectores sociales, políticos y económicos.

4.1 Sector empresarial y las empresas especializadas en ciberseguridad

Las medidas de ciberseguridad se han convertido en una necesidad y en un negocio para las grandes corporaciones que se especializan en tecnologías y desarrollo de software que mitiguen las ciberamenazas. Cuyos costos de inversión ascienden a cantidades millonarias que solo grandes empresas y países desarrollados pueden acceder. Aquí nos encontramos ante el surgimiento de una nueva problemática, el monopolio de la

[20] En primer lugar define a la guerra como un acto de violencia que intenta obligar a nuestro oponente cumplir nuestra voluntad. Plantea tres postulados o condiciones que debe se deben cumplir para ser un acto de guerra: (1) elemento de violencia, (2) instrumental, se utiliza fuerza física y violencia para compeler al adversario y (3) objetivo o intención política (Mehan 2014).

[21] Uno de los casos más mediáticos es el conflicto entre Corea del Norte y Corea del Sur, en el que se ha encontrado que existen cientos de ciberataques contra Corea del Sur ocasionando pérdidas económicas de $805 millones de dólares. Dando lugar a que los periódicos de las dos Coreas especulen sobre las preparaciones militares de cada país para realizar más ataques del sobre el otro (Mehan 2014).

ciberseguridad, en el que, el conocimiento y sus herramientas se convierten en bienes comercializables y poco accesibles para todo público. Una lucha entre el valor comercial privado de la ciberseguridad y las necesidades gubernamentales para reducir las ciberamenazas, El escenario futuro que se debe considerar cuando se habla del mercado de la ciberseguridad y que podría afectar a muchos sectores de la sociedad, inclusive en las políticas internas de un país.

Para el 2018 el gasto mundial en programas de seguridad ascendió a $114 mil millones de dólares, y se calcula que para el 2021 llegue hasta $6 trillones de dólares (Cybersecurity Ventures 2019). Una cifra alarmante que sigue en crecimiento e impacta a las economías de las instituciones públicas y privadas. Además, se estima que alrededor del 32% de las empresas y el 22% de las organizaciones benéficas o recipientes han detectado violaciones o ataques a sus sistemas de ciberseguridad. Siendo las empresas más grandes, las proclives a recibir mayores ciberataques.[22] Pues, éstas al tener mayores ingresos económicos, como entidades financieras o comerciales, se convierten en objetivo de los ciberdelincuentes para robar información y atacar los sistemas que los beneficie económicamente.

Esta particularidad ha obligado que las grandes empresas, contraten del mismo modo los servicios de otras grandes cadenas proveedoras de servicios de ciberseguridad y cibernética, a elevados costos. De acuerdo con los informes de eSecurity Planet y Gartner (2020), las mejores empresas en ciberseguridad que se han posicionado a nivel mundial son: Fortinet (California-EUA) con ingresos anuales de $2,15 mil millones de dólares; KnowBe4 (Florida–EUA); seguida de CISCO (California-EUA) $49,33 mil millones; Splunk (California-EUA) 1,27 mil millones; Microsoft (Washington-EUA) $110,360 mil millones, e IBM (New York-EUA) 77,898 mil millones.

Muchas de estas empresas se encuentran en Estados Unidos, a excepción de Sophos que se origina en Reino Unido, cuyas ganancias son billonarias y operan en diferentes partes del mundo. Ofrecen múltiples productos a organizaciones públicas y privadas, especialmente Fortinet Secure que ha llegado a más de 21.000 organizaciones por sus innovaciones en firewalls, antivirus, prevención de intrusiones y controles de acceso a la

[22] Por ejemplo, el sector de los servicios de información y comunicación que se estima en un 42% (Cybersecurity Ventures 2019).

red (Robb 2020, párr. 4). No es casualidad que estas mismas empresas estén relacionadas con programas de asesoría y capacitación a instituciones públicas para la generación de políticas públicas en ciberseguridad, que a través de organizaciones internacionales, brindan certificaciones en ciberseguridad.

4.2 Las medidas estatales frente al cibercrimen

La mayoría de países norteamericanos y europeos, especialmente, las grandes potencias económicas se han centrado principalmente por mejorar e implementar medidas de seguridad informáticas como la protección a sistemas y bases de datos de instituciones estatales y gubernamentales. Pues el acelerado crecimiento de las redes criminales y la sofisticación de las ciberataques han obligado a que los Estados recurran al asesoramiento de empresas reconocidas en ciberseguridad y en algunos casos al desarrollo de políticas públicas en ciberseguridad.

En el caso de China, por mencionarlo brevemente, es uno de los países asiáticos que ha llevado adelante una serie de medidas estatales para regular el ciberespacio. Cuenta con una Ley de Antiterrorismo, Ley de Seguridad Nacional y la ley de Criptografía que han sido tildadas de ser polémicas, por la cantidad de restricciones y uso del ciberespacio, especialmente para el sector empresarial. Además en 2017 promulgó la Ley del Ciberespacio que le dota de herramientas en la investigación, regulación y tratamiento del ciberdelito, haciendo que el Estado chino tenga a su disposición el 100% de datos de empresas e individuos (Ramírez 2017).

Según el Índice de Ciberseguridad Global (ICG, 2018), realizado por la Unión Internacional de Telecomunicaciones (UIT) que mide indicadores basados en los niveles de seguridad y protección de datos públicos y privados de varios países del mundo en una escala de 0 a 1. En el ranking de 2018 se encontró liderando Reino Unido con el 0.93, seguido por Estados Unidos con el 0.92 y Francia con 0.91 puntos. En los primeros lugares de América Latina, Uruguay ocupa la posición 51 con 0.68 puntos, México posición 63 con 0.62, Paraguay posición 66 con 0.60, Brasil posición 70 con 0.57, Colombia posición 73 con 0.56, mientras que Ecuador en la posición 98 con 0.36 puntos.

Estas mismas potencias son los lugares de donde provienen la mayor cantidad de amenazas cibernéticas como en Estados Unidos con el 14.5% y Rusia con el 7.27%

(Informe trimestral de Spam de Securelist -2015, Noble 2017). Sin embargo, el rastreo del origen de los ataque aún resulta un proceso complejo debido al uso de programas cibernéticos que utilizan patrones para no ser identificados así como sistemas malware que proveen información de otros ordenadores de diferentes partes del mundo.

Pese a los grandes esfuerzos de empresas que ofrecen servicios de ciberseguridad. Aún se registran diferentes tipos de ataques cibernéticos que van en escalada al mismo ritmo que el desarrollo de las tecnologías y el acceso a conocimientos técnicos sobre la vulnerabilidad de los sistemas. El pasado 30 de octubre de 2019 la planta nuclear de Kudankulam (India) había sufrido un ciberataque que afortunadamente no logró afectar sus operaciones. El hecho llamó la atención de especialistas en ciberseguridad, por cuanto este incidente había sido notificado, por un investigador privado indio especializado en ciberseguridad, tres días antes del ataque. Los gobiernos de India, Corea del Norte y Pakistán descartaron alguna responsabilidad con el ciberataque, pues llegar a determinar o rastrear al actor del cibercrimen requiere no solo programas de detección de patrones de IP sino de cooperación internacional y judicial para determinar su autoría.[23]

La magnitud de este hecho marcó una gran preocupación sobre la fragilidad de los sistemas operativos y el ciberespacio que puede causar una serie de consecuencias sociales, políticas, económicas y ambientales. Si no se toman en cuenta mayores medidas de ciberseguridad, las consecuencias pueden ser inimaginables, ocasionando, que existan mayores ataques a otros tipos de infraestructuras críticas.

4.2.1 La gobernanza de la ciberseguridad

Para Mehan (2014) el trans-nacionalismo en el mundo comercial y el creciente internacionalismo económico, social y político; las infraestructuras y sistemas de la información también han evolucionado, para lo cual la ciberseguridad presenta desafíos que hace una década no se podían avizorar. Propone la fundación de una cultura de la ciberseguridad basada en principios de responsabilidad y ética en el tratamiento de la información y la comunicación, mismos que deben ser aplicados no solo a las grandes corporaciones o instituciones gubernamentales, sino a pequeñas empresas y hogares.

[23] Este incidente no fue el primero en su tipo, hasta la fecha se han registrado más de 20 tipos de ciberataques a centrales nucleares que van desde errores de software a intrusiones en sus sistemas operativos (Campbell y Singh 2019).

La gobernanza de la ciberseguridad implica el manejo de conjunto de políticas y controles internos de la estructura y organización como elementos constituyentes a su gestión. Es decir, políticas integrales y coherentes que permita el desarrollo de su organización, anticipándose a futuros riesgos, a pesar que existe el factor de que todas las tecnologías informáticas y sistemas de seguridad sean vulnerables a cualquier tipo de ataque.

Como se ha visto hasta aquí, no ha sido suficiente implementar medidas de ciberseguridad de forma separada a cada tipo de institución, sino se toma en cuenta el desarrollo de políticas orientadas a la lucha contra el cibercrimen y el enfoque en estas seis áreas que obliga la cooperación interinstitucional en los ámbitos públicos y privados para el desarrollo de estrategias cibernéticas (basado en la propuesta metodológica de Wells, Brewster y Akhgar 2016):

- Especialización de investigadores en temas de ciberseguridad y ciberamenazas.
- Cooperación internacional entre Estados y organizaciones a nivel público/privado
- Medición de capacidad de resiliencia de las sociedades.
- Desarrollo, aplicación e interpretación de los sistemas y políticas legislativas.
- Ampliación de los enfoques de sensibilización, educación y capacitación.
- Desafíos resultantes del ritmo del cambio tecnológico y sus implicaciones.

El desarrollo de estas seis medidas requiere de la convergencia de diferentes áreas de la ciencia, tecnología, informática, políticas, sociales y legislativas, que permitan desarrollar mecanismos integrales de respuesta a posibles ciberataques mediante políticas de ciberseguridad dirigidas a todos los actores: Estados, organizaciones internacionales, corporaciones privadas, pequeñas y medianas empresas, y usuarios comunes.

5. Aplicación del derecho penal en el ciberespacio

La gobernanza de la ciberseguridad y los esfuerzos de implementación de medidas de seguridad cibernética deben ir en conjunto con el desarrollo de una legislación adecuada a la naturaleza del cibercrimen. Sin embargo, estos refuerzos requieren de la cooperación internacional para hacer frente a estos nuevos desafíos globales. Este hecho plantea problemas de jurisdicción y aplicabilidad de la ley nacional a una conducta transnacional.

En temas de legislación, se ha tratado de vincular el derecho tradicional al espacio cibernético, lo que ha dado lugar a la generalización de leyes que no cubren los diferentes tipos de cibercrímenes, al igual que otras legislaciones locales no incluyen al delito informático en sus códigos penales. Los principios tradicionales territorialidad, legalidad y de culpabilidad del Derecho Penal, no tienen cabida en el tratamiento y regulación del cibercrimen (Bajovic 2017):

- Principio de territorialidad. Se afirmó bajo ideas del espacio-territorio del Renacimiento y dio lugar a la concepción de que los delitos cometidos dentro de sus fronteras de los estados nacionales, solo pueden ser juzgados y sancionados dentro de los límites de dicha jurisdicción.

  Este principio es desafiado por las actuales tecnologías de la información y la naturaleza del ciberespacio que no reconoce las fronteras físicas. Sin embargo, existe el principio de extraterritorialidad que permite la coordinación de acciones fuera del territorio, siempre y cuando tenga la aprobación, consenso o acuerdo de las autoridades del país extranjero para proseguir con las debidas acciones en ese territorio. Además, en materia probatoria, este tipo de delitos requiere de expertos y asistencias penales internacionales, lo que hace que sean difíciles de investigar, ya que hasta poder contar con una respuesta certificada de otro estado, los delincuentes pueden escapar, cambiarse del país o borrar la huellas de sus actos.

  Este principio aún sigue en discusión entre académicos y juristas, pues éste se encuentra relacionado con conceptos alineados no solo el espacio, frontera o territorio, sino a conceptos como a la cultura, identidad, y otros factores que enriquecen la complejidad del principio. En este sentido, el significado de territorialidad y extraterritorialidad se enmarcan en su propio contexto y son determinados por su propia jurisdicción y normativa, en el que los Estados definen sus principios de acuerdo a su propia voluntad y la aceptación de aquellos instrumentos normativos universales (Torres 2013).
- Principio de legalidad. Se relaciona con la tipificación de los delitos que se incluya en el código penal, los cuales sólo pueden ser aplicados a partir de la entrada en vigencia de la ley y no con efecto retroactivo, es decir, que las personas no pueden ser sancionadas sino existen tales leyes. Las modalidades del cibercrimen se

desarrollan tan rápidamente que se convierten en una desventaja para las legislaciones, sino se actualizan tan pronto como los nuevos ciberataques. Esto deja un amplio espacio para que los ciberdelincuentes aprovechen de sus vacíos para cometerlas. Tal es el caso del virus *Love Bug* que en su momento no estaba tipificado como delito informático en Filipinas, y su actor no pudo ser sancionado.

- Principio de culpabilidad. Se refiere a la responsabilidad penal del individuo en el cometimiento del delito motivado por una intención criminal. En el ciberespacio se debaten la autoría y culpabilidad de los individuos, en cuyos casos, se ha determinado la existencia de adolescentes perpetuadores,[24] que por curiosidad o negligencia han propagado virus sin ninguna intención criminal. En efecto, en todos los delitos se debaten estos puntos para establecer si deben ser penados, es así que todos los delitos deben contar con acto típico, antijurídico y culpable, y si falta un solo elemento no se los puede considerar como acciones que se encasillen como delitos. En el caso de adolescentes propiamente dichos, estos son semi-imputables, es decir, que son culpables, pero en un menor grado por la conciencia de antijuridicidad de sus acciones. Pueden ser juzgados de acuerdo a lo que permitan sus legislaciones internas ya sea como actos lesivos o penales.[25]

El ciberespacio, el desarrollo de la tecnología y el conocimiento técnico sobre las TIC desafían los principios tradicionales del Derecho Penal. La misma realidad a través de los casos suscitados alrededor del mundo, y el acceso de los individuos al ciberespacio a corta edad, traen a discusión que la normativa existente necesita cada vez más de la renovación de sus conceptos y de sus principios en el tratamiento y regulación del cibercrimen.

Para Koops (2016) se necesita una regulación inteligente que implique dos elementos. Primero, una regulación más flexible, reflexiva y sensible, es decir, el establecimiento de leyes duras y blandas que permitan determinar procesos internos y de regulación y control. En segundo lugar, se requiere de una formulación de leyes a un nivel

[24] Se ha demostrado que el 37% de los ciberdelincuentes tienen entre 17 y 25 años, y el 61% de los hackers han iniciado sus actividades a los 10 y 15 años (Bajovic 2017).

[25] En el caso de niños estos son totalmente inimputables, es decir, que casi todas las legislaciones consideran que, pese a que cometa un delito, su grado de consciencia no permite que pueda entender la magnitud de sus actos, sin embargo, al menos en teoría, tienen la obligación de responder civilmente por los daños causados y los encargados de realizar esta indemnización son sus padres o representantes.

adecuado a la neutralidad tecnológica. Un esfuerzo de armonización que implique la actualización y renovación de leyes al mismo nivel en que la tecnología se desarrolla.

Esta armonización debe ser considerada tanto a nivel nacional como internacional a través de políticas domésticas que adecuen sus legislaciones a los desafíos de la tecnología, sin caer en generalizaciones. En el ámbito internacional existen áreas que aún reciben poca atención para ser clasificada como cibercrímenes como la violación de la confidencialidad, uso de datos falsificados, uso ilícito de instrumentos de pago electrónico, actos contra la privacidad, revelación de detalles de una investigación. Algunas de éstas ya han sido consideradas en legislaciones nacionales, pero no han sido incluidas en convenios internacionales que permitan la cooperación y la normalización de procesos legales a escala global. Lo mismo sucede que estos convenios no sean ratificados por los países y se reserve la aplicación de algunas de sus cláusulas (Viano 2017).

La aplicación del derecho en el ciberespacio implica el claro desarrollo de innovaciones legislativas que se adecuen a las exigencias y desafíos del cibercrimen. En primer lugar requiere comprender los efectos de los ataques cibernéticos como parte de un fenómeno global que dista de las dinámicas sociales, políticas y culturales del mundo físico. Segundo, un esfuerzo sistemático que renueve la doctrina del derecho en la aplicabilidad de leyes en la comisión del delito dentro del mundo virtual o cibernético.

6. El futuro del cibercrimen

Uno de los grandes desafíos en la lucha contra el cibercrimen es el aumento de la tecnología junto con el desarrollo sistemático de nuevos y avanzados ataques cibernéticos. No existe un sistema informático, software o dispositivo que no sea vulnerable a las amenazas desde el internet. Un estudio de Juniper Research,[26] predice que el costo de violación de datos ascenderá a 5 mil millones de dólares en 2024, es decir, un crecimiento anual puede llegar hasta el 11%. Una consecuencia real debido a la introducción de la tecnología y de la inteligencia artificial en cada ámbito de la sociedad que, al mismo tiempo, permitirá el desarrollo de sofisticados medios tecnológicos que vulneren sus sistemas de información y operativos.

[26] Ver reportaje completo en: https://securityintelligence.com/articles/the-future-of-cybercrime-where-are-we-headed/

El mundo virtual está viviendo el desarrollo de megatendencias (Koops 2016) que desafían la lógica del delito tradicional y la manera de ver el mundo. El internet se está configurando como la infraestructura de todo y el espacio de la datificación y almacenamiento de información, que necesita cada vez menos de la intervención humana.

Las redes sociales y la rapidez de la información va cambiando su percepción haciéndolas más dependientes de la tecnología a través del uso de smartphones y dispositivos inteligentes que se adecuan a las necesidades de los individuos. Incluso se habla del surgimiento de una nueva megatendencia como el *Internet of People* sobre la relación existente entre máquina, biotecnología y ser humano. Cuyos límites están a punto de cruzarse y crear una simbiosis entre estos elementos. Un futuro desafío para la integridad física de las personas que pueden ser vulnerables a posibles ataques informáticos por el uso de dispositivos o prótesis informáticos adheridos a sus cuerpos.

Si la tecnología avanza a pasos gigantescos y los riesgos aumentan, es necesario replantear las jurisdicciones y los métodos investigativos que permitan reducir las amenazas cibernéticas. Como se ha mencionado anteriormente, no basta con una legislación interna que tipifique ciertos delitos o de la existencia de leyes especiales (que sí son necesarias), depende de la implementación conjunta de políticas criminales y cibercriminales enfocadas hacia un mismo objetivo, el combate contra toda forma de cibercrimen a través de la armonización de legislación local con normas y procedimientos internacionales, ampliación de la cooperación internacional; creación de unidades especiales de investigación de delitos cibernéticos; implementación de medidas de ciberseguridad en redes domésticas, privadas y públicas; programas de sensibilización y capacitación en una cultura web; y capacitación a investigadores judiciales y estatales en temas de ciberseguridad.

Requiere de la voluntad política y la presión social para exigir que sus gobiernos presenten nuevas propuestas políticas públicas que articulen lo jurídico, social, económico, legislativo en el ámbito nacional e internacional para el tratamiento del cibercrimen. Se trata de converger esfuerzos hacia un mismo objetivo y en abrir lazos de cooperación y asistencia técnica para la investigación, capacitación e implementación de políticas cibercriminales

Capítulo segundo
Regulación y tratamiento del cibercrimen

1. Revisión de los instrumentos internacionales en el tratamiento del cibercrimen

En el ámbito jurídico se debaten temas como el marco normativo nacional frente al internacional para la resolución de casos de cibercrimen que no solo atentan a la soberanía de un país, sino a varios indistintamente de su región o ubicación geográfica. Sin embargo, los Estados no asumen completamente la jurisdiccionalidad de los delitos transnacionales, sólo cuando éstos afectan a sus intereses o se ven inmersos en la problemática. Esta responsabilidad se entrelaza con el asunto de los actores involucrados como del alcance de su legislación. Por tanto, llegar a identificar quiénes son los actores y cuál es su propósito para el cometimiento del delito, sigue siendo el gran problema de trasfondo para las legislaciones, que se limitan a sancionar dentro de sus límites jurisdiccionales.

Frente a este escenario, surge diferentes preguntas como: ¿cuál es el camino adecuado para regular el cibercrimen? ¿La respuesta se encuentra en las legislaciones locales o en la cooperación internacional? ¿Los compromisos asumidos en instrumentos internacionales pueden contribuir al tratamiento del cibercrimen y llegar a un acuerdo?

La cooperación internacional permite enfrentar los delitos cibernéticos pero también puede convertirse en un proceso arduo, para "determinar intereses comunes entre varios Estados no siempre es tarea fácil, menos aún la existencia de una *Civitas* máxima (ideal kantiano), porque no existe una Comunidad Internacional o un Orden Internacional claramente reconocido" (Zúñiga, 2016, 104).

En el contexto global diferentes organizaciones internacionales han propuesto el desarrollo de instrumentos internacionales a través de convenios o tratados que permitan analizar y convenir estrategias contra el cibercrimen. Estos esfuerzos se vieron plasmados por primera vez en 1997 con el trabajo conjunto del G7,[27] que estableció principios para la

[27] Grupo de los 7. Originalmente fueron 8 países pero se excluyó a Rusia en 2014, por la anexión de la República de Crimea Ahora está conformado por: Alemania, Canadá, Estados Unidos, Francia, Italia, Japón y Reino Unido.

protección de las infraestructuras críticas de información y un Plan de Acción contra el cibercrimen (Gercke 2014). Entre los principios importantes tenemos:

- Los países deben tener sistemas de alertas de emergencias en relación a vulnerabilidades, amenazas e incidentes cibernéticos.
- Los países deben promover las asociaciones entre los sectores públicos y privados, para compartir y analizar la información sobre las infraestructuras críticas a fin de prevenir, investigar y responder a los daños o ataques a dichas infraestructuras.
- Los países deben promover la cooperación internacional para proteger infraestructuras críticas de información, mediante: el desarrollo y la coordinación de sistemas de alerta de emergencia, el intercambio y el análisis de información en relación a sus vulnerabilidades, amenazas e incidentes, y coordinación de investigaciones de los ataques a esas infraestructuras de conformidad con las leyes nacionales.

Los principios establecidos por el G7 son un conjunto de recomendaciones que abordan principalmente la cooperación internacional. Se enfatiza en la protección de las infraestructuras críticas de la información ante posibles amenazas, vulnerabilidades e incidentes. Estos invitan a la elaboración de políticas públicas entre diferentes sectores de la sociedad con vistas a armonizar sus legislaciones nacionales con mecanismos de cooperación internacional (asistencia mutua, extradición, procesos judiciales).

En este mismo esfuerzo, en diciembre de 2000, se suscribió la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (UNTOC por sus siglas en inglés), justamente por los desafíos mundiales de las redes criminales que operan en diferentes partes del mundo. Son organizaciones complejas que obligó a las Naciones Unidas a determinar tres protocolos para prevenir, reprimir y sancionar la delincuencia organizada.[28] Para los casos de ciberdelincuencia solamente aplica los relacionados con el

[28] (1) Art. 14 del Protocolo de contra el tráfico ilícito de migrantes. Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones contra la Delincuencia Organizada Transnacional; (2) Protocolo contra el tráfico ilícito de migrantes por tierra, mar y aire, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y (3) Protocolo contra la fabricación y el tráfico ilícitos de armas de fuego, sus piezas y componentes y municiones, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

crimen organizado transnacional (Art. 3), no hay artículos que especifiquen sus sanciones o al menos una sección relativa a los delitos informáticos.

En materia de cooperación internacional hay grandes avances en procedimientos para que los Estados parte puedan realizar solicitudes de intercambio de información o asistencia técnica[2] para el decomiso "del producto del delito, los bienes, el equipo u otros instrumentos" (Art. 13) y para la asistencia judicial recíproca (Art. 18).

Más tarde, debido a las crecientes denuncias de sabotaje y fraude informático, en 2001 la Unión Europea suscribió el Convenio del Consejo de Europa sobre la Ciberdelincuencia o más conocido como el de Budapest (2001). En 2003 se creó un Protocolo adicional a la Convención en Cibercrimen relacionado con actos de xenofobia y racismo difundidos por medios tecnológicos (*APCoC).* Al respecto, no todos los países firmantes ratificaron su adhesión al protocolo adicional.

El Convenio de Budapest se convirtió en un instrumento clave para el diseño de políticas públicas y el fortalecimiento de la cooperación internacional para la lucha contra el ciberdelito, que ha servido de modelo para el resto de legislaciones de otros países. En este instrumento ya se tiene una definición de delito informático, con sus diferentes tipos y modalidades para identificar y sancionar los casos relacionados al ciberespacio.

Para los procedimientos de cooperación internacional se encuentran alrededor de 32 artículos,[29] que especifican las medidas legislativas que cada Estado parte debe adoptar, incluyendo los más importantes:

- Procesos de extradición;
- Principios generales a la asistencia mutua;
- Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables;
- Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público;
- Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico; y
- Red 24/7. Sistema de asistencia inmediata disponible todo el tiempo mediante red de contactos en cada Estado parte.

[29] Se encuentran contenidos en el Capítulo III desde el artículo 22 al 35.

Esta última medida, resulta una de las mejores estrategias para la cooperación internacional y el trabajo investigativo inmediato para identificar a los posibles actores del delito. Sin embargo, esto solo aplica a los países ratificados en la Unión Europea (UE).

La mayoría de países de la UE se encuentran suscritos al Convenio de Budapest, pero también se han sumados otros países no miembros de la UE como Australia, Canadá, Japón, Sudáfrica, Estados Unidos, Cabo Verde, Marruecos, Mauricio, Senegal, Israel, Filipinas y Sri Lanka. En América Latina, los países ratificados fueron Argentina, Chile, Costa Rica, Paraguay, República Dominicana y Panamá.

En el aspecto multilateral se cuenta con la Propuesta de una Convención Internacional contra la Delincuencia Cibernética y Terrorismo (2000) realizada por la Universidad de Stanford, el Consorcio para la Investigación en Seguridad y Política (CRISP) y el Centro para la Seguridad y Cooperación Internacional (CISAC). Un proyecto que a diferencia del Convenio de Budapest presenta una Convención multilateral que plantea la constante actualización de las estrategias de lucha contra el cibercrimen a la par del desarrollo de las tecnologías. Excluye las conductas del Estado frente a casos de autoría en su legislación, pero profundiza y determina las definiciones de ciberterrorismo, infraestructuras de información transnacionales, entre otras, en la aplicación del Convenio.

En 2014 la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB) también desarrolló el Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia, al cual solo México, Guatemala, Nicaragua, Portugal, Perú, Uruguay y Argentina se suscribieron al presente instrumento (UNCTAD, 2015). Está conformado por 20 artículos, entre los principales están los relacionados con actividades de cooperación, diligencias de investigación, solicitudes de cooperación y aplicación según el ámbito geográficos de los Estados partes.

Este convenio tendría el mismo alcance que el de Budapest si consideraran otros aspectos como la Red 24/7, que se convierte en una estrategia eficaz para identificar de forma inmediata a los posibles infractores. Sin embargo, no todos los países iberoamericanos están suscritos a este instrumentos, solamente el 31% son miembros parte. Esta estrategia, solo es posible si se consensuaran nuevos acuerdos en el que todos los

países asuman sus compromisos de forma armónica con el resto de Estados de la región, empezando con sus propias legislaciones.

Para el caso de Ecuador en 2014 modificó su legislación a través del Código Orgánico Integral Penal (COIP), logrando tipificar el delito informático, el acoso sexual y la oferta de servicios sexuales con menores de edad en medios electrónicos, y la información fraudulenta entre otros. Los alcances del COIP en esta materia han sido objeto de críticas por la limitada tipificación de los diferentes delitos que se pueden cometer en el ciberespacio (Albán 2016).

En materia de derechos humanos, también han existido debates alrededor del uso e interceptación de datos personales y privados, así como la vigilancia de las personas a través de medios tecnológicos, en que gobiernos o agencias estatales han hecho uso de estos con el objetivo de velar por la soberanía y seguridad nacional. La existencia de estos instrumentos judiciales como la Ley de Vigilancia de la Inteligencia Extranjera (*FISC* por sus siglas en inglés), expedida por el gobierno de Estados Unidos, ha legitimado que agencias estatales (FBI, CIA) puedan acceder a este tipo de información sin que los ciudadanos lo autoricen o estén informados (Thaman 2017). Tal es el caso de la vigilancia a la empresa china Huawei acusada por fraude bancario y conspiración con la empresa Skycom. Motivo que generó el espionaje a llamadas telefónicas y correos electrónicos de ambas compañías (RT 2019).

Del mismo modo sucede con los convenios internacionales como el Convenio de Budapest que ha sido objeto de denuncia por organizaciones sociales y ONG. Según la Fundación Karisma (2018),[30] se convierte en una oportunidad para interferir en el ejercicio de los derechos fundamentales de los ciudadanos. Pues en el caso colombiano, sus políticas han sido dirigidas desde la ciberseguridad y la ciberdefensa sin tomar en cuenta otros factores sociales y el enfoque de los derechos humanos.

Por lo expuesto, todo instrumento internacional es perfectible y susceptible a diferentes criterios, y es aún más en el campo cibernético, que se presentan múltiples debates sobre los derechos humanos, la libertad de expresión frente a los derechos digitales y el alcance de las legislaciones. Sin embargo, es indispensable plantear los mecanismos de

[30] Organización civil de origen colombiana, orientada en la defensa de los derechos humanos en el internet.

cooperación internacional que permitan, al menos, que los países puedan adaptar sus políticas públicas para regular el ciberespacio y las conductas humanas en ambientes virtuales.

A continuación se realiza un análisis de los esfuerzos de los países latinoamericanos en el tratamiento del cibercrimen, para lo cual se procedió a identificar a los países con mejores estrategias en ciberseguridad, basados en indicadores del Índice Global de Ciberseguridad, frente a los países que tienen mayores vulnerabilidades, ya sea por la ausencia de políticas cibercriminales o en ciberseguridad.

2. Comparación legislativa del cibercrimen en Latinoamérica

Para este análisis se presenta una aproximación metodológica al derecho comparado entre las legislaciones de América Latina en cuanto al cibercrimen. Se organizó un esquema,[31] con categorías que permitan identificar lo siguiente: los sistemas políticos; adhesión o suscripción a instrumentos internacionales y los marcos legales internos a cada país (código penal, leyes y tipificación del cibercrimen). En segundo lugar, se añadieron otras categorías complementarias a su estado de situación: indicadores en ciberataques y ciberseguridad basados en el Informe de la Cumbre Latinoamericana de Ciberseguridad de Kaspersky (julio 2018-julio 2019) y el Índice Global de Ciberseguridad (2018),[32] respectivamente; y las políticas públicas y estrategias implementados para contrarrestar las vulnerabilidades cibernéticas (instituciones públicas de regulación del cibercrimen).

Estas categorías permitieron realizar un mapeo, no solo en cuanto a legislación del cibercrimen, sino, sobre los alcances de los ciberataques y las respuestas de los Estados frente a los mismos, si cuentan con políticas públicas en cibercrimen y ciberseguridad, si está o no tipificado en sus códigos penales. Indicadores que permiten visualizar cómo la región se enfrenta a los desafíos globales del cibercrimen.

---

[31] Se recomienda revisar el Anexo 1, Cuadro comparativo de 17 países latinoamericanos, donde se detallan las particularidades de cada país.

[32] Se recurrieron a estos dos informes porque permitieron analizar a través de sus indicadores la situación de la ciberseguridad en la región. En el caso de Kaspersky, es una de las mayores empresas en ciberseguridad presentes en la región latinoamericana que monitorea los ataques cibernéticos por segundo en cada país Kaspersky (23-29 de enero 2020). https://cybermap.kaspersky.com/es/stats#country=35&type=ids&period=w. En cambio el IGC presenta categorías basadas en la gestión pública para medir los niveles de ciberseguridad. Índice de Ciberseguridad Global 2018. https://www2.deloitte.com/cl/es/pages/risk/revista-perspectivas-4ta-edicion/seccion-2/Indice-Global-de-Seguridad-2018.html

Se identificaron un total de 17 países latinoamericanos, que por motivos de extensión, se analizan solamente los países más vulnerables en comparación con los que tienen mejores estrategias en ciberseguridad. Estos son: Bolivia, Guatemala, El Salvador y Costa Rica frente a las medidas implementadas por Colombia, Argentina, Paraguay, Brasil y Uruguay. Para los países con ausencia de políticas en cibercrimen, se toman en cuenta aquellos que tienen similares legislaciones y mínimos puntajes en los indicadores del ICG. Para los países con mejores estrategias en ciberseguridad se tomaron en cuenta los indicadores del ICG y sus políticas implementadas en cuando al cibercrimen.

Cada uno de los siguientes países se encuentra dentro del *Anexo 1 Regulación del cibercrimen en principales países de Latinoamérica,* con su respectiva información que describe su legislación y sus indicadores correspondientes a ciberseguridad.

Bolivia y Guatemala

Bolivia ocupa la posición 135 del ranking global 2018 en ciberseguridad (0,136 puntaje IGC)[33] y tiene una tasa alta de vulnerabilidad del 66.3% frente a delitos informáticos o cibernéticos, lo cual indica que presenta un nivel bajo en el desarrollo de políticas públicas y estrategias para la regulación y tratamiento del cibercrimen. Solamente cuenta con la tipificación de dos delitos cibernéticos en su código penal a través de la manipulación informática y la alteración, acceso y uso indebido de datos informáticos.

En el marco de la economía digital, y como la mayoría de países suscritos a la Organización Mundial de Comercio (OMC), que pretende regular las transacciones del comercio electrónico, Bolivia cuenta con la Ley N° 164 de Telecomunicaciones en relación a comercio electrónico y firma digital para regular y proteger las tecnologías de la información y comunicación y el aspecto radioeléctrico. No se especifican los delitos informáticos, como tal, pero a través del artículo 17 creó el Comité Plurinacional de Tecnologías de Información y Comunicación (COPLUTIC) que podría convertirse en un esfuerzo por vigilar el ciberespacio.

Por su parte, y no lejos del caso boliviano, Guatemala sí se encuentra suscrito al Convenio de la COMJIB, lo que le ha llevado a modificar su código penal para tipificar el

[33] Índice de Ciberseguridad Global 2018 se basa en 25 indicadores agrupados en cinco categorías: legal, técnico, organizacional, creación de capacidad y cooperación. Evalúa cada año a los Estados parte de la Unión Internacional de Telecomunicaciones UIT, siendo cero (0) la escala más baja y uno (1) la más alta.

delito informático en cuanto al robo de información y propiedad intelectual. Sin embargo, se ubica en la posición 112 del ranking global de ciberseguridad y la posición 17 del ranking regional. Sus indicadores sugieren un nivel bajo en ciberseguridad y una insuficiente formulación de políticas cibercriminales.

Se han mencionado estos dos países por su posición en los últimos puestos del ranking regional de ciberseguridad, no obstante sus políticas cibercriminales son diferentes. Según lo revisado, en el cuerpo normativo de Bolivia no está suscrito a algún instrumento internacional específico sobre cibercrimen y aún, así tiene los mismos resultados que Guatemala, que sí posee un convenio en ciberseguridad. Por tanto, la pregunta que surge, es por qué las políticas guatemaltecas y los esfuerzos de implementación de aquel instrumento internacional (COMJIB) no han sido suficientes para frenar los ataques cibernéticos, considerando que, en éste solo están suscritos 7 países de la región latinoamericana. Por tanto, su alcance aún es limitado y la cooperación regional es insuficiente.

El Salvador y Costa Rica

Presentan las mismas similitudes que los casos arriba mencionados, salvo que Costa Rica está suscrito al Convenio de Budapest y al de la COMJIB. Además cuenta con la Sección de Delitos Informáticos del Organismo de Investigación Judicial (OIJ) y la Ley Nro. 8148 para reprimir y sancionar los delitos informáticos, contemplados en su código penal. Sin embargo, es uno de los 128 países con mayores ataques cibernéticos y se encuentra en la posición 115 del ranking global de IGC.

Costa Rica cuenta con una legislación apropiada armonizada con instrumentos internacionales, pero no con las medidas cibercriminales apropiadas que incluyan políticas públicas orientadas en la ciberseguridad y el trabajo conjunto entre lo público y lo privado. No se está contemplando el conjunto de intereses políticos, sociales y económicos que permitan responder a las necesidades de todos los ciudadanos, pues sus indicadores siguen presentando resultados negativos a pesar de su normativa.

En el caso de El Salvador, es necesario resaltar que es un país que ha vivido en constates crisis políticas y civiles, que ha sacudido sus estructuras institucionales.[34] Entre ellas, el combate a la delincuencia y en especial el cibercrimen, no ha logrado superar sus objetivos. En el campo cibernético, en 2016 logró expedir una Ley Especial contra los delitos informáticos ante el acceso indebido a sistemas informáticos y violación de la seguridad del sistema (entre los más destacados), pese a ello, no dispone de una institución que investigue los casos de cibercrimen, lo que le ha llevado a que se ubique en una de las últimas posiciones del ranking global y regional. Por tanto su nivel de ciberseguridad es baja y cada semana sufre más de 370.000 ataques web.

Colombia, Argentina y Paraguay

La institucionalidad y la constante actualización de normas son claves para la regulación del cibercrimen. Sin embargo, la mayoría de países latinoamericanos, han dejado la responsabilidad de vigilar y monitorear al ciberespacio, en manos de unidades policiales no especializadas que trabajan con las mismas figuras penales que el crimen tradicional. Frente a ello, los tres países en mención sí han logrado crear unidades especializadas en cibercrimen o ciberseguridad, y están suscritos al Convenio de Budapest (Colombia, fue uno de los últimos países que se adhirió a este instrumento). Entre las medidas de institucionalización, Colombia creó el Centro de Capacidades para la Ciberseguridad de Colombia (C4) de la Policía Nacional como medida para enfrentar al cibercrimen. En su marco legislativo, contempla la Ley 1273 para tipificar diferentes delitos informáticos desde la interceptación de datos hasta la transferencia no consentida de activos.[35]

En el caso argentino, éste ha modificado su código penal mediante el desarrollo de leyes como: ley de Protección de Datos Personales (Ley 25326) – año 2000; ley de Propiedad Intelectual (Ley 11.723); ley de Delitos Informáticos (Ley 26.388) año 2008; y Ley contra el *Grooming* (Ley 26.904) – año 2013.

[34] En el siguiente artículo se puede tener una visión más clara de la situación salvadoreña: "El Salvador vive una situación como la que lo llevó a la guerra civil". https://elpais.com/internacional/2018/05/18/actualidad/1526673541_527795.html

[35] En 2018 presentó un Proyecto de Ley que actualiza las nuevas modalidades del ciberdelito.

Este conjunto de leyes y la implementación de estrategias en ciberseguridad a través del Ministerio de Modernización de la Nación Argentina, el Plan de ciberseguridad y ciberdefensa y el Programa Nacional de Infraestructuras Críticas, han contribuido a que Argentina se ubique en la *posición 11 de ranking regional*, es decir, en un nivel medio de ciberseguridad.

Paraguay presenta mejores estrategias que Argentina en cuanto a ciberseguridad, ubicándose en el puesto *número 5 del ranking regional* (0,603 puntaje IGC). Cuenta con la Unidad Especializada en Delitos Informáticos del Ministerio Público, institución que hace posible el seguimiento y detección de amenazas y vulnerabilidades cibernéticas.

Además posee una variada lista de delitos informáticos tipificados en su código penal como la alteración de datos, el sabotaje de computadoras; operaciones fraudulentas por computadoras; alteración de datos, etc. con penas privativas de libertad de 1 a 5 años o multas respectivas, de acuerdo a la gravedad del delito.

Uruguay

No cuenta con leyes específicas en delitos informáticos y tampoco tipificados en su código penal, pero si está suscrito al convenio de la COMJIB. Curiosamente se ubica en el *puesto 3 del ranking* regional de ciberseguridad (0,681 IGC), siendo Estados Unidos y Canadá, los que encabezan el primer y segundo lugar de esta lista de países.

La particularidad de Uruguay, radica en la intervención pública y desarrollo de estrategias enfocadas en ciberseguridad a través de instituciones como el Departamento de Delitos tecnológicos de la Jefatura de Policía de Montevideo y el Centro Nacional de Respuesta a Incidentes de Seguridad Informática. Unidades especializadas en el tratamiento del cibercrimen.

Brasil

Representa la mayor economía de Latinoamérica y ocupa la posición 6 en el ranking regional de ciberseguridad. Ha implementado políticas públicas para la regulación del cibercrimen mediante la modificación del código penal, la expedición del Marco Civil de Internet en 2014 y la Ley 12737, exclusiva para delitos informáticos.

En cuanto a cooperación internacional, no está suscrito al Convenio de Budapest ni al COMJIB, mantiene una red interinstitucional para coordinar la ciberseguridad del país a través del Comité Gestor de Internet (CGI); el Ministerio de Comunicaciones Ministerio de Ciencia, Tecnología e Innovación; y el Grupo de Trabajo de Seguridad en Redes, medidas que le han permitido hacer frente a los delitos informáticos, sin embargo, es la figura de extraterritorialidad que contribuye a realizar investigaciones fuera de su jurisdicción.

Frente a este escenario cuenta con varios Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT)[36] administrados por el gobierno y otros dirigidos por el sector privado. Ayudan en la detección de amenazas cibernéticas para ambos sectores. Además cuenta con la Oficina para la Represión de la Delincuencia Cibernética que trabaja con un laboratorio forense digital para la investigación de este tipo de delitos, instalado en cada estado brasileño.

En este contexto, paradójicamente en el mundo del ciberespacio: mientras más desarrollado sea el país, mayores son las amenazas cibernéticas. Brasil presenta el 64.4% de vulnerabilidad y ocupa el puesto número 1 en el ranking global 2018 de *phishing*, y el número 7 de países mayormente atacados en el mundo. Las amenazas se dirigen al sector financiero, siendo el mercado uno de los más afectados.

El trabajo que realiza Brasil en cuanto a ciberseguridad se evidencia de forma multilateral a través de la generación de políticas públicas estatales, legislación específica en cibercrimen y la especialización forense de delitos informáticos, los cuales han permitido desarrollar esfuerzos conjuntos de protección a infraestructura crítica y también privada.

Leyes especiales de otros países

En los casos de Chile, Venezuela y El Salvador, cuentan con una Ley Especial de delitos informáticos, siendo Chile, el único país de este grupo, suscrito al Convenio de Budapest y que presenta un nivel medio de ciberseguridad (puesto 0.47), los otros dos, tienen altas tasas de vulnerabilidad (70,4% Venezuela) por la ausencia de políticas públicas

[36] Esta información se puede ampliar en Ciberseguridad ¿estamos preparados en América Latina y el Caribe? Informe seguridad 2016 presentado por el BID y OEA.

en ciberseguridad y cibercriminalidad, siendo propicios a mayores ataques web y de robos a través de correos electrónicos.

En 2018 Chile presentó un proyecto de ley que derogue la Ley 19.223 y tipifique nuevos delitos informáticos, sin embargo, aún no ha sido aprobado por el actual órgano legislativo chileno.

3. La regulación del cibercrimen en Ecuador

Los desafíos globales de la delincuencia y los nuevos enfoques en el tratamiento legislativo nacional e internacional dieron lugar a la renovación del marco legal y penal de la sociedad ecuatoriana. Así, por mandato de la Constitución de Montecristi (EC 2008, art 424), se debía unificar el cuerpo normativo del sistema penal que incluya: el Código Penal de 1938,[37] el Código de Ejecución de Penas de 1982,[38] y el Código de Procedimiento Penal de 2000,[39] dando lugar al desarrollo del Código Orgánico Integral Penal (COIP) que entró en vigencia en 2014.

Desde el aspecto preventivo, se propuso la Estrategia Nacional de Ciberseguridad en colaboración con el Banco Interamericano de Desarrollo y la consultora NRD *Cyber Security* (en elaboración), bajo directrices y coordinación del Ministerio de Telecomunicaciones. Se encuentra en una fase de elaboración para lo que se solicitó una entrevista con funcionarios de la institución, sin embargo, esta fue rechazada.

También se creó el Centro de Respuesta a Incidentes Informáticos del Ecuador (EcuCERT),[40] institución que permite monitorear el ámbito de las telecomunicaciones y del internet. Actualmente se puede reportar incidentes mediante su página web para recibir asistencia y respuesta a los usuarios solicitantes (empresas y ciudadanos). Funciona como elemento de seguridad cibernética que da seguimiento a las posibles amenazas y vulnerabilidades a las redes informáticas del Ecuador.

Aunque es una iniciativa institucional que refuerza la lógica de ciberseguridad, esta solamente se enmarca en la prevención y capacitación técnica, y como órgano de control a

[37] Desde su vigencia sufrió 46 reformas.
[38] Reformado 10 veces.
[39] Reformado 14 veces.
[40] En el marco de aplicación de la Ley de Telecomunicaciones se creó esta institución, a cargo de la Agencia de Regulación y Control de las Telecomunicaciones.

los prestadores de servicios de telecomunicaciones. En investigación forense informática, pocos son los avances, en Ecuador se cuenta con la Fiscalía de Patrimonio Personal que da atención a este y otro tipo de delitos en cuanto a la normativa le permita para sus diferentes fases de investigación. Pese a todos sus esfuerzos, Ecuador se ubicó en el puesto 8 de ranking global 2018 de *phishing* y presenta un nivel bajo en ciberseguridad (0,367 puntaje IGC). Solo en la última semana de enero de 2020 se detectaron 9.993.312 de ataques web.

En este contexto, las amenazas y vulnerabilidades cibernéticas pueden ser diversas, tal como se ha planteado a lo largo de esta investigación, el Estado y el sector privado-empresarial, evidencian diferentes formas de respuesta y son blanco de distintos tipos de amenazas, para lo cual en el siguiente tema, se analizan los tipos de delitos informáticos comunes en Ecuador y su impacto en estos sectores.

3.1 Tipos de amenazas cibernéticas en Ecuador

Con la formulación del Código Orgánico Integral Penal en 2014, Ecuador desarrolló un marco legal que permite hacer frente a las amenazas y vulnerabilidades del internet. Desde su vigencia hasta el 2018 se registraron 1.265 denuncias ingresadas a Fiscalía General del Estado, todas relacionadas con el cibercrimen y de las cuales 1.072 han sido resueltas, es decir, archivadas, desestimadas o dictaminadas, según sea el alcance de la investigación.

Para ser más específicos, en materia penal, el COIP ha incluido un total de quince artículos referentes al delito informático, que hacen alusión a las mismas conductas del delito tradicional, [41] pero en materia propia del ciberespacio se encontraron solamente cinco delitos relacionados a la naturaleza del internet como: revelación ilegal de base de datos; interceptación ilegal de datos; transferencia electrónica de activo patrimonial; ataque a la integridad de sistemas informáticos y acceso no consentido a un sistema informático.[42]

Los objetivos de este tipo de delitos pueden estar dirigidos tanto al Estado como al sector privado o empresarial. En el caso del Estado ecuatoriano se han tipificado ciertos

[41] Delitos tradicionales cometidos en la web: Art. 103. Pornografía con utilización de niñas, niños y adolescentes (inciso 1); Art. 178.- Violación a la intimidad; Art. 190.- Apropiación fraudulenta por medios electrónicos; Art. 211.- Supresión, alteración o suposición de la identidad y estado civil; Art. 298.- Defraudación tributaria.

[42] En 2019 se presentó el proyecto de Ley de Protección de Datos para poder actualizar y tipificar nuevos delitos informáticos pero aún no ha sido aprobada por la actual Asamblea Nacional.

delitos informáticos como el acceso no consentido a un sistema informático, telemático o telecomunicaciones; ataques contra la integridad de sistemas informáticos; y delitos contra la información pública reservada legalmente. En Ecuador, pueden llegar a ser sancionados con pena privativa de la libertad de cinco a siete años. Si es información pública reservada y compromete la infraestructura de la seguridad estatal, el funcionario relacionado con este hecho será sancionado con una pena de hasta diez años.

Según la base de datos proporcionado por el Consejo de la Judicatura, desde el 2014 hasta el 2018 se han encontrado trece denuncias ingresadas en Fiscalía General del Estado con respecto al acceso no consentido a un sistema informático, telemático o telecomunicaciones, es decir sistemas que puedan afectar este tipo de infraestructuras críticas.

Los funcionarios públicos que estén relacionados a este tipo de delitos, tienen mayores sanciones, por cuanto, su facilidad de acceso les permite vulnerar sus sistemas. Sin embargo, cualquier intromisión a estas infraestructuras, estarían comprometidos otros individuos que pueden cometer estas acciones desde cualquier parte del mundo y su sanción, en caso de ser identificado, solamente tendría una pena de cinco años.

Este fenómeno forma parte de las acciones cometidas por el ciberterrorismo, cuyos objetivos se dirigen, justamente, a causar daños graves a infraestructuras críticas del Estado y a la seguridad pública. Si no se amplían los alcances de estos tipos de delitos, muchos actores no estatales pueden vulnerar estos sistemas y salir impunes. Al respecto, Ecuador tampoco está suscrito a ningún instrumento internacional relacionado con el cibercrimen, por lo cual, identificar y sancionar al perpetrador del delito en otra jurisdicción, es una acción compleja y difícil de aplicar.

En Ecuador se han registrado un total de doce denuncias sobre el ataque a la integridad de sistemas informáticos (EC COIP, art. 232). En lo concerniente al Estado, solamente se tiene un caso ingresado que compromete a servicios públicos o vinculados a la seguridad ciudadana, cuya sanción es la privación de la libertad de cinco a siete años. El alcance de este delito incluye desde el diseño, venta, distribución hasta la destrucción de sistemas informáticos, permitiendo que haya una sanción para cualquiera de estas acciones. Cabe recalcar, que éstos también pueden ser cometidos en el sector privado. Sin embargo,

aquí vemos que la legislación aún sigue siendo genérica, a pesar de la diferencia de una mayor sanción si es dirigido a los servicios públicos.

En cuanto a los delitos contra la información pública reservada legalmente se han registrado tres casos, dentro del período 2014-2018, específicamente relacionados con servidores públicos que han utilizado cualquier medio electrónico para su difusión. Sin embargo, solamente se ha denunciado un caso que compromete la seguridad del Estado, y se ha procedido con una sanción de siete a diez años de privación de la libertad al servidor público que incurrió en este delito.[43]

Una de las respuestas del Estado ha sido el carácter punitivo y sancionador contra este tipo de delitos mediante su legislación (COIP, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos). En el ámbito institucional, aún sigue siendo precario, aunque se cuenta con departamentos como la Unidad de Delitos Informáticos de la Policía Nacional del Ecuador y la Fiscalía de Patrimonio Personal perteneciente a la Fiscalía General del Estado, el Comando de Ciberdefensa del Conjunto de las Fuerzas Armadas (COCIBER),[44] han unido esfuerzos para identificar los delitos cometidos en el ciberespacio dentro de sus competencias.

En este aspecto, la Agencia de Regulación y Control de las Telecomunicaciones ha sido la institución que se ha encargado de garantizar el acceso integral a los servicios de las telecomunicaciones y en la identificación de riesgos y amenazas cibernéticas a través del EcuCert. Un centro de respuesta que contribuye a la seguridad de las telecomunicaciones y del uso del internet. La relevancia de este instituto es la colaboración con otros centros de respuesta fuera del país. Sin embargo, la informática forense ha sido desplazada, mayormente al ámbito privado. La capacitación en esta tipo de investigación es dirigida por instituciones educativas privadas.

En universidades como la Escuela de la Policía (ESPOL), Escuela Politécnica Nacional (Centro de Capacitación Continua), por señalar algunas, han desarrollado talleres y cursos de capacitación en computación forense, y en instituciones de posgrado ofrecen

[43] Esta información se encuentra reservada, por lo que se procedió a analizar en el siguiente capítulo, el caso del robo de datos de casi toda la población ecuatoriana, sucedido en el 2019, un acontecimiento competente para análisis de esta investigación.

[44] Defensa de infraestructuras críticas del Estado.

estudios en ciberseguridad como la Universidad Internacional del Ecuador, Universidad Tecnológica del Ecuador, Universidad San Francisco.

Si bien la capacitación debe ser proporcionada por instituciones educativas especializadas, no se debe negar el carácter privado que tiene este tipo de capacitación en Ecuador. El Estado no ha desarrollado una estrategia que garantice la capacitación de los agentes de investigación de este tipo de delitos ni de los operadores de justicia. Por tanto, esta es una de las principales dificultades en la formación de investigadores forenses informáticos que requiere el país para solventar sus necesidades.

Del mismo modo, esto se visibiliza en la inversión en tecnologías y por tanto en ciberseguridad. Según datos del Ministerio de Telecomunicaciones y Sociedad de la Información, desde el 2007 al 2015 se ha invertido siete mil millones de dólares en telecomunicaciones donde el 32.4% pertenece al sector público y el 67.6% al sector privado. Es decir, el sector privado ha tenido una mayor inversión en telecomunicaciones, ya sea por su capacidad financiera como por sus necesidades propias.

A diferencia del sector privado, el Estado se ha enfocado a través de su marco legislativo e institucional. Pues la inversión en TIC o en ciberseguridad ha sido parcial para solventar las necesidades institucionales. Según el índice de ciberserguridad del 2016 (OEA-BID), Ecuador posee un nivel inicial en el desarrollo de una estrategia nacional de seguridad cibernética, y en las normas de desarrollo de software tanto en el sector público y privado.[45]

Para el mercado, o el sector privado (no estatal) se han determinado delitos como la revelación ilegal de datos, la interceptación ilegal de datos y trasferencia electrónica de activo patrimonial, cuya tipificación determinada por el COIP tiene como sanción la pena privativa de libertad de tres a cinco años. En el primer tipo de delitos, según datos de la Judicatura, desde el 2014 al 2018, se han registrado cuatro casos, que pueden incluir la revelación de información registrada en cualquier soporte, informático, y que intencionalmente se han filtrado.

El delito de interceptación ilegal de datos involucra la escucha, desvío, grabación u observación, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático; la alteración, desarrollo, ejecución o venta de sistemas

[45] Ver anexo 2 Ecuador: Indicadores de Medición del índice de ciberseguridad de la OEA.

informáticos, cualquier acción para desvío de una página diferente a la que el usuario acceda; copia, clonación o comercialización de información contenida en algún dispositivo electrónicos soportadas en tarjetas de crédito o débito; y fabricación, distribución o facilitación de materiales para cometer el delito anterior.

Las dos últimas descripciones están relacionadas con las modalidades del ciber-robo, siendo una de las principales amenazas en el ciberespacio junto el *phishing* o el envío de correos spam que roban datos personales para la clonación y venta de tarjetas de créditos. Se han contabilizado seis casos, de los cuales tres se refieren a delitos como la comercialización o clonación de información de tarjetas de crédito. Aquí los perjudicados, son directamente, los consumidores y el público en general, pues el robo de este tipo de información es común en la ciudadanía, pero pocos son los que se atreven a iniciar procesos judiciales.

También se ha registrado un total de trece denuncias en cuanto a transferencia electrónica de activo patrimonial (bienes), que se refieren a la alteración o modificación de un sistema informático para transferir estos activos a otras personas (fines de lucro) e incluye la entrega de información de cuentas bancarias. Estos delitos tienen una sentencia de tres a cinco años. Tanto las empresas como la ciudadanía en general pueden ser afectadas por este tipo de delitos, cuyos fines, son justamente económicos o de lucro para terceras personas.

Estas pequeñas cifras reflejan que no todos los delitos informáticos han sido denunciados o procesados, ya sea por la falta de información sobre la ilegalidad de estos actos, o al complejo proceso judicial para identificar al posible culpable. Motivos por los cuales, se tiene una pequeña base de datos sobre los delitos propiamente informáticos. Sin embargo, las denuncias aquí registradas ingresadas o resueltas significan que posiblemente hayan sido archivadas o desestimados por falta de pruebas.

En este sentido, especialmente el sector empresarial se ha dotado de sus propias herramientas y tecnologías de seguridad informática. De acuerdo con el estudio de Deloitte realizado en Ecuador durante el 2017 sobre la seguridad de la información, casi el 50% de empresas encuestadas no disponen del presupuesto necesario ni con el personal

especializado para cumplir con este tipo de medidas.[46] Del mismo modo, el 60% no dispone de un Centro de Seguridad (SOC por sus siglas en inglés *Security Operation Center*). Es decir, menos de la mitad del sector empresarial, se encuentra preparado para hacer frente a estos delitos informáticos y que puede poner en riesgo la integridad de sus sistemas.

Cuando las empresas no cuentan con sus propias herramientas, debiera el Estado garantizar una seguridad informática, en el caso de Ecuador, de cierto modo se han implementado medidas enfocadas en lo legal y normativo, pero no son sinónimo de políticas de ciberseguridad que permita que las empresas y usuarios se sientan seguros o respaldados.

Por otro lado, el sector empresarial que brinda servicios de ciberseguridad, ha sido mayormente beneficiado, pues se ha convertido en el centro de respuesta y asesoría para el resto de empresas y corporaciones ecuatorianas en materia de seguridad informática. Es así que según, el Catálogo de servicios y soluciones de Ciberseguridad Industrial 2020,[47] en Ecuador existen alrededor de 35 empresas de soluciones (protección de red, monitorización, cumplimiento, control de acceso) y más de 50 empresas especializadas en diferentes servicios como formación, análisis e investigación de mercado, técnico, consultoría, certificación, entre otros.

La mayoría de estas empresas se destacan como proveedores internacionales y multinacionales que asesoran en materia de ciberseguridad, por ejemplo, tenemos la empresa Entelgy, Kapersky Lab, Deloitte, Everis que ofrecen tanto los mismos servicios como soluciones, ubicándose en ambos sectores, público como privado que necesitan de su soporte técnico y asesoría.

A partir de este contexto, encontramos que Ecuador solamente puede acceder a medidas de ciberseguridad a través de proveedores internacionales para proteger sus sistemas informáticos, es decir, el sector empresarial confía sus bases de datos, sistemas informáticos en manos de empresas extranjeras.

---

[46] Estudio realizado en 2017 a cincuenta empresas nacionales y multinacionales de diferentes sectores del Ecuador (públicos y privados). Sus resultados se encuentran en el Libro blanco de la sociedad de la información y del conocimiento 2018.

[47] Recopilado por el Centro de Ciberseguridad Industrial de las actuales empresas que brindan servicios y soluciones, las mismas que pueden ser multinacionales o internacionales que trabajan en el territorio ecuatoriano.

3.2 Proceso de investigación para casos de cibercrimen en Ecuador

Con la derogación del Código de Procedimiento Penal, el COIP incluye en su texto el conjunto de normas y procedimientos ordinarios de aplicación de sanciones a todo delito, añadiendo, los relacionados con el ciberdelito, éste no tiene un tratamiento especial, a excepción del artículo 500 que se refiere al contenido digital, como medio de prueba o soporte para la fase de investigación.[48]

En cualquier caso, y en especial, para el cibercrimen, se puede contar con el trabajo investigativo de peritos, profesionales y/o expertos en la materia (EC COIP, art. 511). El o la fiscal puede solicitar este tipo de informes, junto con el trabajo realizado por la Fiscalía Especializada de Patrimonio Ciudadano de la Fiscalía General del Estado en coordinación con la Policía Nacional del Ecuador. En efecto, no hay unidad especializada, pero a través de estas instituciones se receptan y procesan las denuncias relacionadas a este tipo de delitos (usura, apropiación ilícita, destrucción de Sistema Informático o Red Electrónica).

De alguna manera estas medidas han permitido implementar un proceso un poco diferente al tratamiento del cibercrimen, a pesar, que no se estipule un procedimiento específico. Se cuenta con el procedimiento ordinario que consiste en: instrucción, evaluación y preparatoria de juicio, y juicio.[49]

Es necesario mencionar estas etapas por cuanto los plazos que rigen son claves en el proceso penal. Por ejemplo, solo en la fase investigación previa se determinan los indicios y pruebas hasta dos años desde su fecha de inicio (denuncia). En casos de cibercrimen el tiempo es crucial, y cada segundo es la oportunidad para borrar sus huellas en el ciberespacio. Todo depende del tiempo de denuncia hasta la resolución del fiscal para investigar los hechos del presunto delito y de acuerdo a las pruebas presentadas ante la Fiscalía para iniciar las subsecuentes etapas del proceso penal. Solo hasta ese momento muchos rastros y posibles huellas del perpetrador ya pudieron ser borrados. Aunque existan

[48] En las primeras reglas de investigación se aclara que estos se someterán a análisis mediante técnicas digitales forenses y a cadena de custodia para su valoración.

[49] 1. Fase de investigación previa: hasta dos años desde su fecha de inicio; 2. Etapa de instrucción: hasta noventa días, a excepción de lo determinado en el art. 592; 3. Fase de audiencia de preparatoria de juicio: con elementos suficientes se llaman a audiencia, en un plazo no mayor a cinco días y se efectuará en un plazo no mayor a quince días (art. 600) y; 4. Fase de juicio: debe sustanciarse en un tiempo de hasta 18 días.

las figuras de allanamiento, registro y operaciones encubiertas, todas son disponibles en casos excepcionales y salvo el o la fiscal lo autorice.

Si seguimos esta línea de investigación y el debido proceso penal para determinar posibles actores nacionales o extranjeros en un posible caso de cibercrimen, se puede considerar también diversas diligencias extraterritoriales (EC COIP, art. 407), teniendo la potestad de realizar otro tipo de reconocimientos o acciones fuera del país que le contribuyan a su investigación. Sin embargo, todo esto dependerá de la decisión del o la fiscal encargado del caso, para comunicarse con la contraparte y en solicitar su autoridad para iniciar las investigaciones pertinentes.

Ahora qué sucede con los casos de cibercrimen en que no se ha podido identificar a los actores y las pruebas son insuficientes. Según el COIP, se podrá prescribir o archivar si no se ha cumplido con los plazos establecidos o no se cuentan con los elementos suficientes para formular los cargos. Se solicitará el archivo de caso, sin perjuicio de solicitar su reapertura cuando aparezcan nuevos elementos siempre que no esté prescrita la acción (EC COIP, art. 417 y 586).

Esto posiblemente, nos da una idea en cómo rige el COIP en posibles casos de cibercrimen, cuyos alcance es limitado, no solo por su tipificación, sino por el procedimiento penal que se aplica de forma genérica a delitos tradicionales y delitos cibernéticos. No se cuenta tampoco con protocolos alternativos que permitan una rápida acción judicial y policial en este tipo de casos, dejando a la sospecha y criterio del o la fiscal a cargo, y que en muchos casos, éstos son archivados o desestimados por falta de elementos convincentes y de prueba para la acción penal.

En el siguiente capítulo se presentan aquellos casos relacionados directamente con el ciberespacio, y que es necesario revisar cuál ha sido el enfoque investigativo en delitos informáticos y la vulnerabilidad de éstos.

Capítulo tercero
Estudios de casos

En este capítulo se analizan dos vertientes que han sido transversales en los delitos informáticos en Ecuador. La primera, los casos relacionados a la jurisdicción nacional, regional, transnacional e internacional que pone en debate el rol de los actores estatales y no estatales en el cometimiento de este tipo de delitos. La particularidad de este primer análisis a breves rasgos es la situación política y coyuntural que marca diferentes perspectivas sobre la jurisdicción internacional y nacional.

La segunda vertiente tiene que ver con un análisis en cuanto al tipo de delitos relacionados con la revelación ilegal de datos, suplantación de identidad y la violación a la intimidad. Aunque estos son distintos, en esta investigación se plantea un caso en el que se relacionan estos tres actos ilícitos que no solo vulneraron los derechos individuales sino colectivos, frente a las medidas de protección del Estado ecuatoriano.

Para los siguientes casos se recurrió al uso de reseñas cronológicas, se sugiere revisar los anexos 3, 4 y 5, donde se presentan las descripciones de cada caso en orden cronológico, gracias a los aportes de noticias, artículos, entrevistas e investigaciones previas que permitieron esclarecer los diferentes sucesos.

1. Análisis de casos relacionados a la jurisdicción nacional, regional, transnacional e internacional vs. actores estatales y no estatales

Este primer análisis plantea un caso que ha sido fuertemente discutido por el derecho internacional, los derechos humanos y la libertad de expresión, bajo diferentes figuras legales, académicas, especialmente políticas. Me refiero al caso del informático australiano Julian Assange y el ciudadano sueco Ola Bini. Este último implicado en el caso por su relación cercana a Assange.

1.1 Caso Julian Assange

Julian Paul Assange es un informático de origen australiano que se desempañaba como periodista y programador,[50] sin embargo, su notoriedad y labor polémica se debió a la fundación del portal digital WikiLeaks. Un sitio web que difundió y filtró, de manera anónima, una gran cantidad de información reservada de varios gobiernos, principalmente contra países como Estados Unidos. Se estima que existen alrededor de quinientos mil documentos confidenciales, entre esos, cuatrocientos mil relacionados con la Guerra de Irak y noventa mil sobre la guerra de Afganistán (Forn, 2015).

Estas no fueron las únicas revelaciones en el sitio web, desde su fundación en 2007, el equipo de Julian Assange ha difundido información sensible que ha puesto en evidencia a muchos secretos de Estado y encubrimiento de sucesos, especialmente alrededor de las guerras en Medio Oriente por la incursión de Estados Unidos. Para tener claro de la importancia de estas filtraciones de información se presenta una breve cronología, para lo cual se solicita revisar detenidamente el Anexo 3,[51] de los principales eventos de la persecución y encarcelamiento de Assange a consecuencia de esta actividad que le llevó a ser conocido como el mayor hacker de la historia en la revelación de datos. Defendido por unos como activista político y otros como delincuente informático.

Análisis del caso

Si se revisa minuciosamente la cronología de eventos que dieron vuelco a la detención de Julian Assange, se evidencia un primer momento del posicionamiento internacional de un periódico digital con intenciones políticamente claras en revelar y divulgar de manera anónima secretos de Estado. En segundo lugar, se hacen divulgaciones de los procedimientos militares y la incursión de Estados Unidos en Medio Oriente, teniendo en cuenta que no solo contaba con fuentes de información claves en la revelación de documentación gubernamental, entre ellas, el soldado Bradley Manning, quien posteriormente fue arrestado por el gobierno estadounidense por divulgar esta información (Forn, 2015).

[50] A pesar que se formó en matemáticas, filosofía, neurociencia y física, se autoeducó en informática.

[51] La cronología presentada se basa en aportaciones de la investigación de Marta Forn (2015) y en reportajes de periódicos locales e internacionales.

Desde el nacimiento de WikiLeaks, mucha información ultrasecreta y confidencial no solo causó molestias entre los países involucrados.[52] En una de las divulgaciones de Wikileaks, expuso al presidente ecuatoriano Lenin Moreno a través de documentos como INA Papers, que sugerían la creación de empresas *offshore* o fantasmas y el incremento de su patrimonio provocando preocupación en el primer mandatario (Gozzer 2019). Además expuso a líderes políticos a través de evidencias fehacientes (correos electrónicos, documentos, fotos, videos) que revelaron el manejo del poder y sus principales intereses políticos, tanto en ocultar información como los hechos que transgredían derechos humanos.

Tras estas divulgaciones, Assange se convirtió en un personaje público exponiéndose a la querella de detractores y defensores de la libertad de expresión y de prensa, popularizado por revelar documentos oficiales. Sin embargo, mientras avanzaba su popularidad, en 2010 se abre una investigación contra Assange por acoso sexual. Un cargo judicial que fue escalonando hasta que llegó a manos de autoridades británicas para dar paso a su extradición a Suecia. Paralelamente, un tribunal secreto estadounidense presentó cargos contra Assange por las intromisiones a sus archivos digitales confidenciales.[53].

Dado este contexto, se da inicio a un complejo proceso judicial, en el que ahora Assange debía buscar refugio para no ser extraditado a Estados Unidos (se debe tener en cuenta que aún no se revelaban oficialmente las intenciones de enjuiciamiento por parte del país norteamericano). Para el 2012 consigue el asilo político en la Embajada de Ecuador en Londres, como un recurso que facilite su salida del país británico. Esta condición dio comienzo a un nuevo revés diplomático en tratar de solucionar la situación de Assange pero duró siete años hasta su detención en 2019.[54]

Durante el transcurso de estos años, surgió una transición diplomática, que en 2013 empezaron a establecer negociaciones entre los cancilleres de Ecuador y Reino Unido (Forn, 2015). Sin embargo, no lograban llegar a un acuerdo, debido a la situación política

[52] Entre los afectados se encuentra principalmente Estados Unidos, como el de Debbie Wasserman, presidenta del Comité Nacional Demócrata, quien tuvo que renunciar a su cargo, debido a la filtración de audios que revelaban donaciones a funcionarios a cambio de favores (CNN 2016).

[53] Información obtenida del portal de la BBC News (11 de abril de 2019). https://www.bbc.com/mundo/noticias-internacional-47897043

[54] Para mayores detalles de la detención de Assange, se recomienda revisar el artículo de la revista digital La Vanguardia (11 de abril de 2019): https://www.lavanguardia.com/internacional/20190411/461587338442/julian-assange-detenido-londres.html

que enfrentaba cada país frente a los compromisos asumidos con Estados Unidos, ya que, es posterior a estas conversaciones que se plantea el Brexit (consulta popular 2016)[55] y la posibilidad de establecer relaciones con el país norteamericano.

A partir de este enclave en las negociaciones, Assange empieza a revelar las presunciones de que Estados Unidos tiene planes de enjuiciarlo bajo la Ley de espionaje o terrorismo. Frente a estos temores, se siguen publicando información de Estados, entre ellos los correos electrónicos de Hilary Clinton. Este hecho fue decisivo para que se retire el servicio de internet a Assange dentro de la embajada ecuatoriana, inhabilitándole de sus pronunciamientos políticos.[56]

Las publicaciones y revelaciones de información fueron periódicas, lo que siguió llamando la atención de medios de comunicación y líderes políticos. Sin embargo, este hecho no ayudó a las negociaciones entre ambos países. Una salida posible era la nacionalización de Assange concedida en diciembre de 2017 por el gobierno ecuatoriano para establecer el estatus de agente diplomático. Para lo cual las autoridades británicas denegaron el otorgamiento de esta condición a Assange, llevándolo nuevamente a otra encrucijada diplomática.

Tras ocho meses del gobierno posicionado por Lenin Moreno y a pesar de la nacionalización ecuatoriana de Assange concedida por su propio mandato, empiezan a existir malestares en su gobierno por las intromisiones de Assange en asuntos políticos de otros países y por su colaboración con hackers rusos. El cambio en su política se evidenció con el retiro del asilo y la entrega de Assange a la policía británica en abril del 2019.

A mediados del 2019 se mostraron las intenciones e intereses de los países involucrados. Primero Ecuador con la entrega de Assange, en medio de conversaciones comerciales y políticas con Estados Unidos (reuniones con el vicepresidente Mike Pence en julio de 2019).[57] Segundo, Reino Unido que tras el Brexit se empezaron a intensificar las relaciones políticas y comerciales con Estados Unidos, pieza clave para no conceder el

[55] Se puede revisar el artículo de la BBC (2019) para comprender la posición de Gran Bretaña y Estados Unidos en cuanto a los fines comerciales en: https://www.bbc.com/mundo/noticias-internacional-46901065

[56] Otra cronología del caso Assange se puede recurrir al portal de noticias DW en el siguiente enlace: https://www.dw.com/es/cronolog%C3%ADa-del-caso-assange/a-46723957

[57] Para mayores detalles de la reunión bilateral entre los dos países puede revisar el comunicado de la Embajada de los Estados Unidos en Ecuador (U.S. Mission Ecuador 2019): https://ec.usembassy.gov/es/dialogo-politico-bilateral-ecuador-estados-unidos-comunicado-conjunto/

salvoconducto de salida del país británico y probablemente extraditarlo a EE.UU. Tercero, el propio país norteamericano y el principal actor estatal, que a un mes de la detención de Assange publicó la formulación de dieciocho cargos incluyendo la Ley de Espionaje, cuya pena podría ser de ciento setenta y cinco años de cárcel.

Este conjunto de estrategias a base del establecimiento de compromisos entre los países involucrados (Ecuador, Gran Bretaña), tuvieron como único propósito no permitir que se divulgue más información estatal que comprometa su permanencia en el poder, tanto en el caso ecuatoriano (a partir de la divulgación de los documentos denominados INA PAPERS del patrimonio del Presidente Lenin Moreno en paraísos fiscales) como en el británico (Brexit) y revele los intereses ocultos detrás de secretos de Estado o información legítimamente reservada.

A la luz de los delitos informáticos, los aspectos legales de detención de Assange y su intromisión en asuntos de Estado, dependerá de la jurisdicción de cada país, en el que se estipule qué es un acto lícito o ilícito, qué tipo de delito cometió, qué se considera como delito informático o información reservada. Sin embargo, frente a todo ello, no se debe olvidar que el proceso judicial contra Assange inició con una demanda de extradición sueca por acoso sexual, a lo que fue sumando otras figuras judiciales por no cumplir con ciertas normas de presentación ante los tribunales británicos. Proceso que fue enmarañándose a medida de que WikiLeaks iba publicando más información reservada. No fue hasta 2010 que apenas existió una demanda secreta iniciada por Estados Unidos contra Assange y que recién pudo ser conocida de manera incompleta,[58] donde fue considerado como un delito de revelación de información reservada.

1.2 Caso Ola Bini

Ola Metodius Martin Bini es un programador informático de procedencia sueca, cuya experiencia profesional se especializa en seguridad informática, criptografía y privacidad. Ha sido reconocido como el mejor encriptador en su haber. Llegó a Ecuador en 2013 para dictar talleres relacionados a estos temas.

[58] El Universo (2020). "Departamento de Justicia de EE. UU. refuerza cargos contra Julian Assange". https://www.eluniverso.com/noticias/2020/06/25/nota/7884003/justicia-estadounidense-refuerza-cargos-contra-julian-assange

Este joven programador de 37 años ha sido relacionado inmediatamente con el caso de Assange por haber establecido contacto con el fundador de WikiLeaks. Para entender la problemática y las particularidades de su proceso investigativo abierto por las autoridades ecuatorianas, es necesario revisar en el tiempo la serie de eventos que partieron desde su arribo a Ecuador.

Para el análisis del presente caso se recomienda revisar su cronología correspondiente al Anexo 4. Con el propósito de tener un mejor acercamiento al caso también se examinó la comunicación enviada por el Grupo de Trabajo sobre la Detención Arbitraria de la Organización de las Naciones Unidas (ONU) sobre el "Llamamiento Urgente Conjunto de los Procedimientos Especiales",[59] el expediente digital que se encuentra subido en la Consulta de procesos Sistema Automático de Trámite Judicial Ecuatoriano (SATJE),[60] así como también las publicaciones de periódicos digitales y entrevistas de Ola Bini a medios de comunicación.

Análisis del caso

Para esta investigación es relevante un análisis de su proceso penal, puesto que este caso aún no ha sido resuelto, ni tampoco tiene una fecha de juicio debido a la complejidad del proceso judicial. Además se encuentra lleno de eventos que indican principalmente un interés político. Según su abogado Carlos Soria, desde el momento de su detención hasta la formulación de sus cargos fueron realizados de manera arbitraria e irregular. Las pruebas y evidencias encontradas no eran suficientes para que sea detenido. Pues si revisamos la cronología, no existía una orden de detención más que una dirigida a un ciudadano ruso y que tras varios intentos de comunicación era imposibilitado de contactarse con su abogado.

Una de las primeras observaciones al caso, es el hecho de la detención de Ola Bini a horas de la entrega de Assange a autoridades británicas. Sin embargo, el móvil que llevó a la detención de Ola Bini es la vinculación que diera a conocer autoridades ecuatorianas por posibles ataques informáticos de presuntos aliados de Assange en Ecuador. Coincidentemente o no Bini, estaba por salir del país hacia Japón.

[59] Referencia: UA ECU 7/2019, en relación a la detención de Ola Bini.

[60] Número de proceso: 17282201901265. http://consultas.funcionjudicial.gob.ec/informacionjudicial/public/informacion.jsf

En este caso, el principal actor está representado por el Estado, por tanto el delito informático relacionado con el ataque a la integridad de los sistemas informáticos fue un recurso para ser usado en contra de un ciudadano extranjero con conocimientos de informática. No obstante, el hecho de no poseer una orden de detención, y su principal denuncia se basó en declaraciones de la Ministra del Interior permite deducir que su detención fue arbitraria y viola con el procedimiento legal ecuatoriano.[61]

Siguiendo la línea de tiempo es durante el día de su detención que se ejecuta una orden de allanamiento que determinó como evidencias a dispositivos tecnológicos que, como programador informático, se encontraban en su vivienda. Sin embargo, en la audiencia de formulación de cargos se le acusa de ataque a la integridad de sistemas informáticos, con base a los gastos excesivos de internet y el material allanado. Consecuentemente se dicta prisión preventiva y congelamiento de sus activos.

Después de setenta días de cárcel, finalmente se aprueba el recurso de habeas corpus para que Ola Bini pueda salir de prisión preventiva que no se sustentaba en evidencias fehacientes que den cuenta del cometimiento de aquel delito. En este ámbito a días de finalizar su instrucción fiscal, se realiza una reformulación de cargos contra Bini en el que se le acusa de acceso no consentido a un sistema informático. Ahora los principales acusantes son el fiscal del caso y el representante legal de CNT por haber ingresado a redes privadas de las empresas CNT, Petroecuador y de la SENAIN.[62]

Esta acusación se basó en una conversación por WhatsApp con Marco Arguello (quien tenía una relación contractual con CNT) en el que se envía la imagen del sistema de CNT con fallas de seguridad en los servidores que utilizan el programa TELNET (2015).[63] Con este nuevo antecedente, la instrucción fiscal finaliza. Su juicio ha sido postergado varias veces y aún no tiene definida la fecha debido a la situación de suspensión de causas no flagrantes por el estado de emergencia sanitaria.

---

[61] Estas denuncias públicas se hicieron a través de las cuentas de twitter del Ministerio de Gobierno, para constancia de ello, aún se encuentran en las redes: https://twitter.com/mingobiernoec/status/1118642800919232514?lang=bg

[62] Según declaraciones Bini al periódico El Comercio, la reformulación de cargos se hizo dos días que acabara la instrucción fiscal, "No tuvimos los 30 días preceptivos constitucionales para preparar la defensa". https://www.elcomercio.com/actualidad/ola-bini-fiscalia-juicio-ciberseguridad.html

[63] Ola Bini. “Análisis de la filtración de Novaestrat”. https://autonomia.digital/es/privacy/2019/09/28/analysis-novaestrat.html

Esta serie de eventos ha hecho posible identificar dos actores: el acusante en la figura del Estado y el acusado en la figura de un ciudadano extranjero, llamado aquí por el aspecto legal como "delincuente informático" y amigo de J. Assange. Pues a semanas, de la reformulación de cargos, el presidente Moreno en una entrevista declara públicamente que Ola Bini ha intervenido en la política de Ecuador y del mundo.[64] Una declaración que evidencia que Bini seguirá en el ojo público y de las autoridades ecuatorianas. Es así que para enero de 2020 se difunden imágenes en las que la casa del programador sueco se encuentra vigilada por presuntos policías.

Estas últimas declaraciones, luego de las emitidas por la Ministra del Interior, y las acusaciones del representante de CNT en la audiencia de reformulación de cargos. Solamente revela la existencia de una maquinaria estatal frente a un individuo en calidad de ciudadano extranjero, que desde cualquier punto de vista, es o puede desembocar en una persecución política hasta que el juicio tenga lugar, y finalmente se dictaminen cargos en su contra para llevarlo nuevamente a la cárcel.

El caso de Ola Bini no solamente revela las irregularidades de su proceso investigativo penal, sino el rol estatal frente a sucesos relacionados con los delitos informáticos que no son fácilmente comprobables en Ecuador. Especialmente porque muestra la vulnerabilidad de los sistemas de seguridad del país frente a posibles ataques informáticos que pueden ser realizados en cualquier parte del mundo Pues, en la comunicación de Bini a M. Arguello (evidencia de su "culpabilidad"), [65] indica que tanto empresas públicas como privadas siguen utilizando un sistema de seguridad obsoleto denominado TELNEL, entre estas CNT, la empresa pública y la más grande en telecomunicaciones del país.

Ahora lo que entra en claros cuestionamientos, es la veracidad del testimonio de Ola Bini, en que si esa información solamente fue transmitida a Arguello para fines profesionales, o que haya ingresado a éste y otros sistemas para su propio beneplácito Sin embargo, aún no es posible tener acceso al expediente completo ni a las evidencias

[64] Declaraciones en entrevista realizada por el periodista Omar del Rincón en el programa CNN Español. https://cnnespanol.cnn.com/video/lenin-moreno-ecuador-julian-assange-ola-bini-entrevista-fernando-del-rincon-conclusiones/

[65] Se refiere a la comunicación mantenida mediante mensajes de whatsapp, que fueron capturados mediante cámaras de seguridad en un ascensor. Puede revisar la entrevista realizada por el canal digital de youtube La Posta (24 junio 2019). https://www.youtube.com/watch?v=z1MEgQRhvSc

encontradas que se presentarían en el juicio futuro donde se sustente cualquiera de las dos tesis.

Teniendo en cuenta este panorama, el Estado ha presentado recursos que, indiscutiblemente de ser legales o no, juega con mayor ventaja frente a un individuo, dentro de su propio marco judicial e internacional que lo soporte. En este caso, las acciones precedidas son legitimadas por ser Estado, para determinar una causa judicial, en nombre de preservar la llamada seguridad nacional y la información reservada, como uno de sus principales intereses.

2. Análisis de casos relacionados a la revelación ilegal de datos y violación a la intimidad de la población ecuatoriana

Para analizar estos delitos informáticos en cuanto a la revelación ilegal de datos y la violación a la intimidad, se tomó el caso reciente del robo de datos de los ecuatorianos en 2019 que involucra a dos denuncias de fuga de información masiva de datos personales. Se utiliza una reseña cronológica para la resolución y análisis de este caso complejo.

2.1 Robo de datos personales de los ecuatorianos

Esta serie de eventos sucedió en el 2019 (ver anexo 5) simultáneamente con el arresto de J. Assange y Ola Bini, trayendo al debate la complejidad de los delitos informáticos y los desafíos globales que enfrenta Ecuador.

Análisis del caso

El mundo digital es un espacio cada vez más complejo que supera la capacidad del mundo físico para manejar redes de información y procesar grandes algoritmos matemáticos e informáticos. Por ello, se ha convertido en nuestro principal recurso para el almacenamiento de información y el manejo de gigantescas bases de datos sensibles y privados. Con la transformación del mundo digital, toda nuestra información está disponible a un clic en las redes sociales, aplicaciones y programas frecuentes que usamos en nuestros dispositivos móviles. Bancos, supermercados, tiendas, instituciones públicas y privadas, confían su información en empresas de seguridad informática.

Ecuador también trabaja con estas empresas, sin embargo no todas. El 2019 fue un año clave que evidenció las vulnerabilidades y fallas de seguridad informáticas, que venía arrastrando desde años anteriores,[66] especialmente en las instituciones públicas. Es así que para el mes de septiembre se hizo pública la denuncia de la exposición de información sensible de casi diecisiete millones de personas, incluidos siete millones de menores de edad, en un servidor alojado en Miami.[67]

Esta información trascendió la opinión pública debido a la publicación de un twitter de los informáticos israelíes Noam Roten y Ran Locarque detectaron estas fallas de seguridad a inicios de septiembre y las denunciaban a las autoridades ecuatorianas. [68] Sin embargo, la noticia no explotó sino es por la gravedad de la información revelada, que incluía datos personales, cuentas bancarias, dirección domiciliaria, números de placas, historial laboral, todas provenientes de bases de datos de instituciones públicas y bancarias. Por ejemplo información del Instituto Ecuatoriano de Seguridad Social, Registro Civil, Corporación Nacional de Telecomunicaciones, Ministerio de Educación, entre otras instituciones.

La particularidad de este hecho a más de la filtración de datos sensibles, es el involucramiento de la empresa de seguridad Novaestrat que no contaba con las mínimas seguridades para proteger la información y que la haya alojado en Miami. La cuestión aquí radica en que no solo se confiaron esas bases de datos a una empresa privada, sino que tampoco hubo un seguimiento por parte de Ecuador para garantizar que efectivamente se está protegiendo la información personal de sus ciudadanos. Además, resulta curioso, que su representante legal en el país haya sido absuelto de la justicia ecuatoriana, y aún no se identifique a los responsables de esta fuga de información. Hasta el momento la empresa señalada aún no ha dado nombres ni mayores declaraciones para la investigación del caso.

[66] Declaraciones emitidas de Ola Bini en la entrevista realizada por el canal digital La Posta (24 junio 2019).

[67] Ola Bini realizó un "Análisis de la filtración de Novaestrat" donde se expone una cronología y su punto de vista sobre el robo de información. https://autonomia.digital/es/privacy/2019/09/28/analysis-novaestrat.html

[68] El Comercio (24 septiembre 2019). https://www.elcomercio.com/actualidad/venta-datos-ecuatorianos-investigadores-informatica.html

En medio de estos sucesos, el propio Ministro de Telecomunicaciones Andrés Michelena,[69] reveló que solamente el 26% de las instituciones públicas guardan su información en sitios seguros, lo que se deduce que la mayoría de éstas no cuentan con las mínimas seguridades, exponiendo información personal a la vista de diferentes hackers, empresas privadas (fines comerciales o publicitarios) y de organizaciones criminales que pueden hacer uso de estas bases de datos para cualquier propósito. No obstante, las empresas privadas también pueden ser víctimas de fuga de información, pues en el mismo mes se hizo pública otra denuncia de robo de datos como por ejemplo seguros privados, sueldos del mes de agosto entre otra información confidencial. Este hecho vincula a otra empresa de seguridad que también se encuentra en investigaciones.[70]

El robo de datos de todos los ecuatorianos revela las vulnerabilidades de la información digital, las pocas y escasas medidas de seguridad y privacidad de las instituciones públicas y privadas. Especialmente el sector público que no ha tomado las acciones mínimas de ciberseguridad para prevenir futuros robos y filtración de datos. Ante esta situación en 2019 se presentó a la Asamblea Nacional el proyecto de Ley de Protección de Datos Personales que hasta el momento sigue en discusión.[71]

La necesidad de contar con una legislación adecuada forma parte del resto de acciones que debe tomar el Estado para salvaguardar la información, así como la creación de políticas de ciberseguridad que responda a las exigencias mínimas de protección de datos personales y públicos. Pues con esta fuga de información, las acciones posteriores resultan tardías debido a que todos los ciudadanos seguimos expuestos al ojo y escrutinio de diferentes actores, organizaciones u otros individuos que tienen acceso a nuestra información. En este sentido, el gobierno ecuatoriano decidió que todas las bases de datos de las instituciones públicas sean migradas y administradas por una sola empresa pública, en este caso CNT. Sin embargo, ya no se puede asegurar que toda la información publicada aún sea mal utilizada por otros actores.

---

[69] Entrevista Rafael Bonifaz, experto en seguridad informática (18 septiembre 2019). http://www.pichinchauniversal.com.ec/experto-en-seguridad-informatica-migrar-datos-a-servidores-de-cnt-no-es-la-solucion/

[70] El Telégrafo (25 septiembre 2019). https://www.eltelegrafo.com.ec/noticias/politica/3/gobierno-denuncia-robo-datos

[71] El actual Ministro entregó dicha ley como parte de las acciones para combatir la intromisión maliciosa de información pública (MINTEL, 2019). https://www.telecomunicaciones.gob.ec/ministro-michelena-entrego-proyecto-de-ley-proteccion-de-datos-personales-al-presidente-de-la-asamblea-nacional/

Ecuador, al igual que otros países de la región (Bolivia, Colombia, Costa Rica, El Salvador), enfrenta el mismo problema de establecer una armonía legislativa con sus políticas de ciberseguridad. En los casos de Bolivia y Colombia, como se revisó en el segundo capítulo, evidencian niveles bajos de ciberseguridad por cuanto sus políticas públicas no están orientadas bajo una estrategia propia en ciberseguridad y cibercriminalidad. El caso presentado de Ecuador, reveló justamente la despreocupación del Estado por invertir y mejorar la infraestructura digital y de ciberseguridad de sus instituciones públicas y privadas así como la de sus ciudadanos. Se demostró que existen grandes desafíos cibernéticos por enfrentar y aún por resolver en cuanto al robo de información sensible de la población ecuatoriana.

El *phishing* o robo de datos es cada vez más frecuente en la región latinoamericana. Ecuador ocupa el puesto número ocho del ranking regional, a diferencia de Brasil que ocupa el primer lugar y cuenta con una amplia legislación específica en delitos informáticos. Para el caso ecuatoriano, luego de este grave suceso en 2019, el ciudadano común es más propenso al robo de datos e inclusive a la suplantación de identidad. Solamente en la última semana de enero de 2020 se detectaron 9.993.312 ataques en la web (donde existe la posibilidad de que cada semana incremente),[72] es decir, el país sigue siendo blanco de delitos informáticos, y si no se toman las medidas necesarias, muchos o casi todos los ecuatorianos serán los afectados, incluida la integridad de miles de niños que también fueron expuestos en este robo masivo de información.

[72] Las Ciberamenazas se pueden visualizar en tiempo real de cualquier país del mundo, a través de la página web de Kaspersky. Estas cifras corresponden a la semana del 22 al 28 de enero de 2020. https://cybermap.kaspersky.com/es/stats#country=136&type=ids&period=w

Conclusiones

El ciberdelito es un fenómeno global que afecta a todas las naciones del mundo a pesar de la existencia de una normativa legal o de un cuerpo legislativo que intente regular los delitos en el ciberespacio. Países de la región latinoamericana como Ecuador se enfrentan a los mismos desafíos globales que conciernen a otras naciones, sin embargo, son las capacidades y las formas de respuesta del Estado frente a los delitos informáticos que marcan los niveles de seguridad informática y protección de los datos privados y confidenciales de sus ciudadanos. Al no existir una política doméstica que regule estos delitos informáticos, los ciudadanos se encuentran expuestos a la impunidad de estos actos ilícitos, y a la vulnerabilidad de sus datos personales.

Desde la perspectiva de las relaciones internacionales y a la luz del análisis comparativo de las legislaciones latinoamericanas, se evidencia que las normativas y los cuerpos legales no son suficientes para controlar el ciberespacio sino se desarrollan políticas públicas enfocadas en materia de ciberseguridad, en investigación forense informática; políticas que fomenten en sus ciudadanos una cultura cibernética, o permitan el trabajo coordinado entre instituciones públicas y privadas para, intercambiar experiencias en cuanto al manejo de bases de datos. Al contrario, se presentan muchos casos en países latinoamericanos como el abandono y la despreocupación total del mundo cibernético por parte del Estado, permitiendo que el sector privado desarrolle sus propias estrategias de seguridad informática sin ningún tipo de regulación estándar que garantice la privacidad de los datos.

En este sentido, cuando se analiza la participación de las empresas privadas en la ciberseguridad, éstas tampoco demuestran ser garantía de protección de datos personales y sensibles, pues al no existir una política clara de seguridad informática, estos actores pueden hacer uso de bases de datos reservados sin ningún tipo de control estatal, o trasladar información a diferentes lugares sin ninguna autorización, como fue el caso de la empresa Novaestrat que presuntamente provocó el robo de información de los ecuatorianos en el año 2019.

La ciberseguridad es un campo que debe ser tratado por diferentes acciones estales y estrategias inteligentes que articulen lo público y lo privado, empezando por la formulación de políticas domésticas. Si se parte de esta premisa, la cooperación internacional sería una de las formas de respuesta inmediata en el que el Estado podría mejorar su capacidad de control y regulación del cibercrimen dentro y fuera de su jurisdicción. Sin embargo, para pensar en una cooperación internacional se debe trabajar en políticas públicas en cuanto a ciberseguridad y protección a la privacidad de los ciudadanos, requiere nuevas propuestas políticas que articulen lo jurídico, social, económico y legislativo y, que éstas respondan a los actuales desafíos globales del cibercrimen. Pues una de los principales problemáticas de Ecuador es la elaboración de políticas en ciberseguridad que blinde la integridad de la información de todas las instituciones públicas y privadas.

Cuando se analiza la particularidad de Ecuador frente a los desafíos globales del cibercrimen, no es la misma capacidad de respuesta del Estado para resolver los posibles conflictos del ciberespacio. La tipificación del delito informático y su inclusión en el Código Penal en 2014, ha sido un gran paso en la legislación ecuatoriana, sin embargo, los procesos de instrucción fiscal y las fases de investigación son cruciales para identificar a los actores del delito. Para el caso de Ecuador, los procesos aún siguen siendo dilatados en el tiempo y no todos los casos han sido investigados, en gran parte por las pruebas insuficientes, las pocas denuncias presentadas y la desarticulación entre las instituciones públicas y privadas que trabajan de manera individual y poco coordinada para investigar este tipo de delitos.

En el análisis de los tres casos ecuatorianos que coincidentemente tuvieron como desenlace en el año 2019, reveló el juego de intereses políticos y el rol del Estado frente a la investigación de los delitos informáticos. En primer lugar, la situación de Julian Assange expuso el cambio de política exterior en la diplomacia de los países involucrados en cuanto a la toma de decisiones para la protección de un activista político que revelaba secretos de Estado e información confidencial de diferentes países del mundo. Este caso se tornó en un asunto político a través de la intervención de distintos actores, principalmente aquellos que se vieron afectados por la revelación de información: Estados Unidos, Gran Bretaña y Ecuador.

No obstante, fuera del complejo proceso judicial y diplomático que debatían la forma de salida de Assange de Londres, este informático representaba para el Estado un enemigo que no podía ser fácilmente neutralizado, debido al involucramiento de varios actores. Sin embargo, este juego de intereses políticos que lo empezó todo, posterior al cambio de administración del gobierno ecuatoriano, dio por concluido el asilo político y consecuentemente el inicio de su proceso de extradición a Estados Unidos.

En los dos últimos casos, el de Ola Bini y el robo de bases de datos de la población ecuatoriana, se determinó que existen graves fallas en los sistemas de seguridad informáticos del Ecuador, incluidos los sistemas de las instituciones públicas. Sin embargo el factor político ha sido clave en la toma de decisiones para iniciar un proceso de investigación contra los actores implicados en estos dos casos. En el primero por su asociación con Julian Assange y el segundo porque implicaba la revelación de información pública y reservada que manejaban varias instituciones públicas, cuya responsabilidad recaía en la figura del Estado ecuatoriano. Lamentablemente, estas motivaciones políticas se han centrado en defender solamente el papel del Estado, y poco en las acciones estratégicas que se requieren para salvaguardar las bases de datos robadas que ahora pueden ser vulneradas por cualquier persona que tenga acceso a ellas.

Estos casos puntuales evidenciaron el bajo nivel de ciberseguridad que Ecuador presenta en la región a partir de las escasas medidas de seguridad informática que la mayoría de las instituciones públicas implementan para albergar los datos de la población ecuatoriana, la ausencia de políticas públicas en cibercrimen y deficientes estrategias en ciberseguridad. Los casos analizados como se presume el de otros, revelan la falta de preocupación del Estado frente a la infraestructura digital de las instituciones públicas y privadas, poniendo en riesgo la integridad de la población ecuatoriana.

Bajo este contexto, es necesario que se reformule, en primer lugar, una política pública en ciberseguridad, un cuerpo normativo coherente a la situación ecuatoriana a través de una ley de Protección de Datos Personales en conjunto con la institucionalización del control y regulación de los delitos informáticos. También es importante la creación de una institución autónoma al Estado y del mercado, que permita proteger los datos privados y personales de los ecuatorianos, sin la intervención de intereses privados o particulares que puedan hacer uso de éstos para beneficio propio.

Analizar los desafíos globales resultantes del ciberdelito, en particular para las legislaciones latinoamericanas, permitió identificar las dificultades gubernamentales y estatales para hacer frente al ciberdelito. Se ha determinado, que a pesar de existir una normativa que regule el cibercrimen no es suficiente en la mitigación de este tipo de delitos. Resulta que los países con mejores niveles en ciberseguridad han desarrollado políticas públicas enfocadas en la especialización de unidades de investigación de delitos informáticos, en programas de educación y cultura digital dirigidos a toda la ciudadanía, en capacitación de operadores de justicia y una serie de estrategias que se van actualizando al corto y al largo plazo dentro de sus planes de ciberseguridad. Un programa conjunto de medidas y políticas que se alimentan del sector público y privado.

Para Ecuador representa un largo camino que recorrer, las experiencias vividas en los últimos años ha permitido, al menos, identificar que la ciberseguridad es un eje importante en la administración de la infraestructura crítica y de información que requiere de todos los esfuerzos y la voluntad política para enfrentar estos desafíos globales. Pues, mientras se siga subestimando el mundo del ciberespacio, mayores serán los desafíos que enfrente el país y en consecuencia, un mayor número de afectados en la ciudadanía, que podrían ser víctimas de incontrolables delitos informáticos

Obras citadas

Albán, Juan Pablo. 2016. *Regulación de Internet y derechos digitales en Ecuador*. Quito: Universidad San Francisco de Quito.

Bajovic, Vanja. 2017. "Criminal Proceedings in Cyberspace: The Challenge of Digital Era". En *Cybercrimen, organized crimen and Societal Responses*, compilado por Emilio C. Viano, 87-102. Cham: Springer International Publishing Switzerland.

BBC News Mundo. 2019. "Quién es Julian Assange, el polémico fundador de WikiLeaks arrestado en la embajada de Ecuador y que EE.UU. considera una amenaza". 11 de Abril. https://www.bbc.com/mundo/noticias-internacional-47895702.

Bermúdez, Ángel. 2019. "Brexit - cierre del gobierno: por qué Reino Unido y Estados Unidos acabaron sumidos en crisis políticas tan graves y quiénes son los grandes beneficiados", 17 de Enero. https://www.bbc.com/mundo/noticias-internacional-46901065.

Campbell, Alexander, y Vickram Singh. 2019. "Lessons from the cyberattack on India's largest nuclear power plant", Bulletin of the Atomic Scientists, 14 de Noviembre. https://thebulletin.org/2019/11/lessons-from-the-cyberattack-on-indias-largest-nucl/?utm_source=Newsletter&utm_medium=Email&utm_campaign=Newsletter11142019&utm_content=NuclearRisk_Cyberattack_11142019.

Chawki, Mohamed, Ashraf Darwish, Mohammad Ayoub, y Sapna Tyagi. 2015. Cybercrimen, digital forensics and jurisdiction. New York: Springer International.

CNN. 2016. "Las 10 filtraciones más importantes de WikiLeaks en sus 10 años". 04 de Octubre. https://cnnespanol.cnn.com/2016/10/04/las-10-filtraciones-mas-importantes-de-wikileaks-en-sus-10-anos/.

CJ Consejo de la Judicatura 2018. "Base de datos Sistema Automático de Trámite Judicial Ecuatoriano (SATJE)". Base Excel de datos estadísticos de delitos informáticos 2014-2018.

Cybersecurity Ventures. "2019 Official Annual Cybercrime Report". Herjavec Group. A. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf.

EC COIP. 2014. *Código Orgánico Integral Penal*. Asamblea Nacional. Registro Oficial, Suplemento 180.

Edwards, Susan S.M. 2017. "Cyber-Grooming Young Women for Terrorist Activity: Dominant and Subjugated Explanatory Narratives". En *Cybercrime, Organized Cryme and Societal Responses. International Approaches*, de Emilio C. Viano, 23-46. Cham: Springer.

Forn Bosch, Marta. 2015. "El Asilo Político: El caso Assange". Tesis de Grado en Derecho. Facultad de Ciencias Sociales: Universitat Abat Oliba CEU.

Fundación Karisma. 2018. *Convenio de Budapest: Aplicación en Colombia frente a derechos humanos*. Bogotá: Derechos digitales.

Gamba, Jacopo. 2010. "Panorama del derecho informático en América Latina y el Caribe". Colección Documentos de proyectos. Comisión Económica para América Latina y el Caribe (CEPAL). https://core.ac.uk/download/pdf/38672044.pdf.

Gercke, Marzo. 2014. Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica. UIT.

Global Voice. 2013. "Filipinas: Denuncian ley contra el cibercrimen como Ley Marcial Cibernética". Global Voice, 28 de Enero. https://es.globalvoices.org/2013/01/28/filipinas-la-ley-contra-el-delito-cibernetico-denunciada-como-ley-marcial-cibernetica/.

Goodman, Marc. 2010. "International Dimensions of Cybercrimen". En *Cybercrimes: A Multidisciplinary Analysis*, editado por Sumit Ghosh y Elliot Turrini, 311-339. Heidelberg: Springer.

Gozzer, Stefania. 2019. BBC News Mundo. "Arresto de Julian Assange, fundador de WikiLeaks: por qué supone la "ruptura definitiva" de Lenín Moreno con la herencia de Rafael Correa". 11 de Abril. https://www.bbc.com/mundo/noticias-america-latina-47893539.

Holt, Thomas, y Adam Bossler. 2016. "Applications of criminological theory to cybercrimes". En *Cybercrime in progress: theory and prevention of technology enabled offenses*, compilado por Thomas Holt y Adam Bossler, 65-105. New York: British Library Cataloguing in Publication Data.

INEC, Instituto Nacional de Estadísticas y Censo. 2015. *Módulo de TIC de las Encuestas de Manufactura y Minería, Comercio*. Quito: INEC.

Kaspersky. 2019. "Informe de la Cumbre Latinoamericana de Ciberseguridad de Kaspersky". Kaspersky. Acceso el 12 de diciembre. https://www2.deloitte.com/cl/es/pages/risk/revista-perspectivas-4ta-edicion/seccion-2/Indice-Global-de-Seguridad-2018.html#, 2018-2019.

———. 2020. "Ciberamenazas. Mapa en tiempo real". Kaspersky, Acceso el 23 de enero. https://cybermap.kaspersky.com/es/stats#country=136&type=ids&period=w

Koops, Bert-Jaap. 2016. "Megatrends and Grand Challenges of Cybercrime and Cuberterrorism Policy and Reseach". En *Combatting Cybercrimen and Cyberterrorism. Challenges, Trends and Priorities,* recopilado por Babak Akhgar y Ben Brewster, 3-15. AG Switzerland: Springer Nature.

La Posta. 2019. "Café la Posta: Ola Bini, amigo de Assange". La Posta, 24 de junio. https://www.youtube.com/watch?v=z1MEgQRhvSc.

Mehan, Julie E. "Cyberwar, Cyberterror, Cybercrime and Cyberactivism". Ely, UK: It Governance Publishing; Second Edition, 2014.

Ministerio de Telecomunicaciones. 2020. "Ministro Michelena entregó proyecto de Ley Protección de Datos Personales al presidente de la Asamblea Nacional". Mintel. Acceso el 12 de junio. https://www.telecomunicaciones.gob.ec/ministro-michelena-entrego-proyecto-de-ley-proteccion-de-datos-personales-al-presidente-de-la-asamblea-nacional/.

Neto, Joana. 2017. "Social Network Analysis and Organised Crime Investigation: Adequacy to Networks, Organised Cybercrime, Portuguese Framework". En *Cybercrime, Organized Cryme and Societal Responses*. International Approaches, recopilado por Emilio C. Viano, 179-200. Cham: Springer.

Noble, Wayne. 2017. "Cyber Armies – The Growth of the Cyber Defence Industry". En *New Perspective on Cybercrime*, editado por Tim Owen, Wayne Noble y Faye Christabel Speed, 63-80. Cham: Palgrave Macmillan.

ONU Asamblea General. *Convención de las Naciones Unidas contra la delincuencia organizada transnacional y sus protocolos*. 15 de noviembre de 2000. 55/25

Organización de Estados Americanos, Banco Interamericano de Desarrollo. 2016. "Ciberseguridad ¿estamos preparados en América Latina y el Caribe? Informe de ciberseguridad". Banco Interamericano de Desarrollo.

Owen, Tim. 2017. "The Problem of Virtual Crimonology". En *New Perspective on Cybercrime*, editado por Tim Owen, Wayne Noble y Faye Christabel Speed, 177-193. Cham: Palgrave Macmillan.

Páez Rivadeneira, Juan. 2010. "Derecho y TICS". Quito: Corporación de Estudios y Publicaciones, 384 p.

Ramírez, David. "Ciberseguridad en China". *Instituto Español de Estudios Estratégicos*, 2017: 8-15.

Robb, Drew. 2020. "Top Cybersecurity Companies". eSecurity Planet. 3 de Enero. https://www.esecurityplanet.com/products/top-cybersecurity-companies.html

RT Russian Today. 2019. "EE.UU. usó la ley de Vigilancia de la Inteligencia Extranjera para espiar a Huawei en secreto". Russian Today, 06 de Abril. https://actualidad.rt.com/actualidad/310889-eeuu-ley-fisa-espionaje-huawei-evidencia-secreto.

Singh, Hardeep. 2019. "20 Cybersecurity and Phishing Statistics That Matter in 2019". Appknox, 3 de abril. https://www.appknox.com/blog/cybersecurity-statistics-2019.

Sofaer, Abraham, Seymour Goodman, Mariano Florentino, y Ekaterina Drozdova. 2000. "Propuesta de una Convención Internacional contra la Delincuencia Cibernética y Terrorismo. Consorcio para la Investigación en Seguridad y Política", Universidad de Stanford: 29.

Thaman, Stephen C. 2017. "The Use of Information and Communications Technology in Criminal Procedure in the USA". En *Cybercrime, Organized Crime and Societal Responses. International Approaches*, recopilado por C. Emilio Viano, 103-134. Washington DC: Springer.

Torres, Henry. 2013. "La extraterritorialidad de la Ley Penal: El principio de justicia universal, su aplicación en Colombia". *Revista Prolegómenos - Derechos y Valores*: 99-115.

Turrini, Elliot, y Sumit Ghosh. 2010. “A Pragmatic, Experiential Definition of Computer Crimes”. En *Cybercrimes: A Multidisciplinary Analysis*, editado por Elliot Turrini y Sumit Ghosh, 3-23. Heidelberg: Springer.

UIT Unión Internacional de Telecomunicaciones. 2018. “Índice de Ciberseguridad Global”. https://www.itu.int/Pages/PageNotFoundError.aspx?requestUrl=https://www.itu.int/en/pages/404.aspx.

U.S. Mission Ecuador. 2019. “Comunicado Conjunto Reunión del Diálogo Político Ampliado Bilateral Ecuador-Estados Unidos". Embajada de Estados Unidos en Ecuador. https://ec.usembassy.gov/es/category/estados-unidos-y-ecuador/.

Viano, Emilio C. 2017. “Cybercrime: Definition, Typology, and Criminalization”. En *Cybercrime, Organized Cryme and Societal Responses. International Approaches*, recopilado por Emilio C. Viano, 3-22. Cham: Springer.

Wall, David. 2001. “Cybercrimes and the Internet”. En *Crime and the Internet*, de D.S. Wall (Ed.), 1–17. New York: Routledge.

———. 2008. “Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime”. En *Information Communication and Society*: 1-33.

Wells, Douglas, Ben Brewster, y Babak Akhgar. 2016. “Challenges Priorities and Policies: Mapping the Research. Requirements of Cybercrime and Cyberterrorism Stakeholders”. En *Combatting Cybercrimen and Cyberterrorism. Challenges, Trends and Priorities*, editado por Babak Akhgar y Ben Brewster, 39-52. AG Switzerland: Springer Nature.

Zúñiga, Laura. 2016. “El concepto de criminalidad organizada transnacional: problemas y propuestas”. *Revista Nuevo Foro Penal* 12 (86): 62-114.

Anexos

Anexo 1: Regulación del cibercrimen en principales países de Latinoamérica

País	Sistema político	Instrumento internacional	Marcos legales			Indicadores en ciberamenazas[73]	Ciberseguridad [74]	Políticas y estrategias
			Código Penal	Leyes	Tipificación del cibercrimen			
1.Argentina	República Fed. Presidencialista	Convenio de Budapest; Convenio COMJIB	Código Penal de la Nación Argentina, vigente desde 1921. Uso de términos: delitos informáticos; comunicación electrónica	- Ley de Protección de Datos Personales (Ley 25326) – año 2000; - Ley de Propiedad Intelectual (Ley 11.723) - Ley de Delitos Informáticos (Ley 26.388) año 2008, -Ley 26.904 - Grooming 2013- Uso de término: delito informático	En el Código Penal se tipifica lo incorporado por las leyes: -Ley 25326. Art. 117 Bis y Art. 154 Bis -Ley 26.388 Art. 128 Art. 153. Violación de Secretos y la Privacidad: Art. 155. Art. 157; Art. 183; Art. 184; Art. 1987; Art. 255 -Art. 131 -grooming	-3.131.268 incidentes -Puesto 15 ranking global de phishing	-Posición 94 en ranking global 2018 -Posición 11 en ranking regional 2018 -Nivel medio en ciberseguridad (0.40 puntaje IGC)	- Ministerio de Modernización -Plan de ciberseguridad y ciberdefensa -Programa Nacional de Infraestructuras Críticas
2. Bolivia	República presidencialista	_____	Código Penal vigente desde 1995. Actualizado en 2010 Uso de términos: datos informáticos	-Ley N° 164, Ley General de Telecomunicaciones y Tecnologías de Información y Comunicación (comercio	En el Código Penal se tipifica: Art. 363 bis. Manipulación informática Art. 363 ter. Alteración, acceso y	66.3% de vulnerabilidad	-Posición 135 en ranking global 2018 -Posición 24 en ranking regional 2018 -Nivel bajo en ciberseguridad	-Comité Plurinacional de Tecnologías de Información y Comunicación -No cuenta con políticas públicas para la regulación

[73] Según el informe de la Cumbre Latinoamericana de Ciberseguridad de Kaspersky (julio 2018-julio 2019).

[74] Índice de Ciberseguridad Global 2018. https://www2.deloitte.com/cl/es/pages/risk/revista-perspectivas-4ta-edicion/seccion-2/Indice-Global-de-Seguridad-2018.html

				electrónico, firma digital) - Acoso cibernético (Código de Niño, Niña Adolescente)	uso indebido de datos informáticos		(0,139 puntaje IGC)	del cibercrimen.
3. Brasil	República Fed. presidencialista	_____	Código penal Modificación o alteración de sistemas informáticos Art. 313 A. Art. 313 B. Uso de términos sistemas informáticos.	- Marco Civil de Internet – año 2014 Ley núm. 12737 – año 2012, exclusivo para delitos informáticos Uso de términos: datos informáticos	En el Código Penal se tipifica Art. 154 A. Invasión de dispositivo informático. Art. 266 interrupción o perturbación de servicio telegráficos, informáticos, Art. 298. Falsificación de datos.	- 64.4% de vulnerabilidad - Puesto 1 ranking global de phishing - Puesto 7 de países atacados en el mundo	- Posición **70** en ranking global 2018 - Posición **6** en ranking regional 2018 - Nivel medio en ciberseguridad (0,577 puntaje IGC)	- Comité Gestor de Internet (CGI) - Ministerio de Comunicaciones Ministerio de Ciencia, Tecnología e Innovación - Grupo de Trabajo de Seguridad en Redes
4. Chile	República presidencialista	Convenio de Budapest	Código penal. Actualización 2011	Ley de 19.223 consta de 4 artículos – año 1993 (Ley Específica) Uso de término: delito informático	En la ley se tipifica Art. 1 Sabotaje informático Art. 2 y 4 Espionaje informático	- Puesto 7 ranking global de phishing	- Posición **83** en ranking global 2018 - Posición **9** en ranking regional 2018 - Nivel medio en ciberseguridad (0,47 puntaje IGC)	- En 2018 se presentó Proyecto de ley que tipifique y derogue la Ley de 19223 - Estrategia Nacional de Ciberseguridad (Coordinación del Sistema Nacional de Ciberseguridad, del Ministerio del Interior y Seguridad Pública) - Instructivo Presidencial de Ciberseguridad para servicios públicos

5. Colombia	República presidencialista	Convenio de Budapest	Código Penal Colombiano Ley 599 de 2000	Ley 1273 - año 2009 Consta de 4 artículos. Se incorporan al código penal	En el Código Penal se tipifica del Art. 269A-al Art. 269J. Interceptación de datos Daño informático Uso de software malicioso Trasferencia no consentida de activos Uso de término: delito informático	- 105.304.886 ataques de malware	- Posición **73** en ranking global 2018 - Posición **7** en ranking regional 2018 - Nivel medio en ciberseguridad (0,565 puntaje IGC)	- Cámara Colombiana de Informática y Telecomunicaciones (CCIT) - Centro de Capacidades para la Ciberseguridad de Colombia (C4) de la Policía Nacional.
6. Costa Rica	República presidencialista	Convenio de Budapest; Convenio COMJIB	Código Penal Violación de Secretos Del art. 195 al 203 Uso de términos: Delitos informáticos	Ley No. 8148 para reprimir y sancionar los delitos informáticos. Se incorporan en el código penal. Uso de término: Delitos informáticos	Art. 196 bis Violación de comunicaciones electrónicas Art. 217 bis.-Fraude informático Artículo 229 bis.- Alteración de datos y sabotaje informático.	- Posición 128 de país más atacado, 262.956 ataques web en una semana[75][76]	- Posición **115** en ranking global 2018 - Posición **19** en ranking regional 2018 - Nivel bajo en ciberseguridad (0,221 puntaje IGC)	- Sección de Delitos Informáticos del Organismo de Investigación Judicial (OIJ)
7. Ecuador	República presidencialista	_____	Código Integral Penal formulado en 2014, Tipificación de delitos informático	Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos (Ley No. 2002-67) Concepto: servicios electrónicos	CP. Art. 104. Pornografía infantil (transmisión por cualquier medio) Art. 178. Violación de la intimidad Art. 190. Apropiación fraudulenta por	- Puesto 8 ranking global de phishing. - Se detectan un total de 9.993.312 de ataques web en la última semana de enero 2020[77].	- Posición **98** en ranking global 2018 - Posición **15** en ranking regional 2018 - Nivel bajo en ciberseguridad (0,367 puntaje IGC)	- Ministerio de Telecomunicaciones - Centro de Respuesta a Incidentes Informáticos del Ecuador (EcuCERT), de la Agencia de Regulación y

[76] Ciberamenazas en tiempo real. Fuente: Kaspersky (22-28 de enero 2020)https://cybermap.kaspersky.com/es/stats#country=136&type=ids&period=w
[77] Ciberamenazas en tiempo real. Fuente: Kaspersky (23-29 de enero 2020) https://cybermap.kaspersky.com/es/stats#country=35&type=ids&period=w

			Uso de términos: Sistemas de información		medios electrónicos Art. 231. Transferencia electrónico de activo patrimonial Art. 211 y Art. 298 falsificación cibernética Art. 229 al Art. 234 Delitos contra la seguridad de los activos de los sistemas de información y comunicación			Control de las Telecomunicaciones (ARCOTEL) - Esquema Gubernamental de Seguridad de la Información (EGSI-2013) - Proyecto de Ley de Protección de Datos -2019 - Elaboración de Estrategia Nacional de Ciberseguridad (BID –Consultora NRD Cyber Security)
8. El Salvador	República presidencialista	_____	Código Penal. Actualización 1997 Art. 238-A Fraude de comunicaciones Uso de términos: sistema de comunicaciones	Ley Especial Contra los Delitos Informáticos y Conexos- año 2016 36 artículos Uso de términos: delito informático, bien jurídico protegido, programa – sistema informático.	En la ley especial se tipifica (más relevantes): Art. 4 Acceso Indebido a Sistemas Informáticos Art. 5. Acceso Indebido a Sistemas Informáticos Art. 9 Violación de la Seguridad del Sistema	- 371.847 ataques web en la última semana de enero 2020[78]	- Posición **142** en ranking global 2018 - Posición **28** en ranking regional 2018 - Nivel bajo en ciberseguridad (0,124 puntaje IGC)	_____
9. Guatemala	República presidencialista	Convenio COMJIB	Código Penal de Guatemala Uso de términos: delitos informáticos.	_____	En el código Penal se tipifica del Art. 274 “A” al 274 “G” y 275. Robo de información y propiedad	- Puesto 10 ranking global de phishing	- Posición **112** en ranking global 2018 - Posición **17** en ranking regional 2018 - Nivel bajo en	- Instituto Nacional de Ciencias Forenses de Guatemala- investigación en delitos informáticos

[78] Ciberamenazas en tiempo real. Fuente: Kaspersky (23-29 de enero 2020): https://cybermap.kaspersky.com/es/stats#country=173&type=ids&period=w

					intelectual		ciberseguridad (0,251 puntaje IGC)	
10. Honduras	República presidencialista	_____	Código Penal de Honduras. Actualización 2019 Art. 389 Propiedad intelectual Uso de términos: delitos informáticos, datos informáticos	Decreto Legislativo 64-2007, de reforma de la Ley de Transparencia y Acceso a la Información Pública. Acuerdo IAIP-001-2008 de 03 de marzo del 2008.- Reglamento de la Ley de Transparencia y Acceso a la Información Pública	En el código Penal se tipifica del Art. 398 al 405 Art. 398 Acceso no autorizado a sistemas informáticos Art. 399 Daños a datos y sistemas Art. 400 Abuso de dispositivos Art. 401 Suplantación de identidad	- Puesto 12 ranking global de phishing		- Instituto de Acceso a la Información Pública (IAIP) - Dirección Nacional de Información Criminal de la Policía Nacional
11. México	República Fed. Presidencialista	Convenio COMJIB	Código Penal Federal (1931) Actualización 2018 Uso de términos: sistemas informáticos	Ley General del Sistema Nacional de Seguridad Pública (ciberseguridad-2009) Ley de Seguridad Nacional (2005) Uso de términos: base de datos; sistemas de información; sabotaje, espionaje	En el código penal se tipifica: Art. 210 Revelación de secretos Art. 211 bis Acceso ilícito a sistemas y equipos de informática	- Puesto 11 de países atacados en el mundo y en el Puesto 13 ranking global de phishing	- Posición **63** en ranking global 2018 - Posición **4** en ranking regional 2018 - Nivel medio en ciberseguridad (0,629 puntaje IGC)	- Unidad especializada en delitos informáticos de la Procuraduría General
12. Panamá	República presidencialista	Convenio de Budapest (2014)	Código Penal de la República de Panamá. Actualizado 2007 Uso de términos seguridad informática	_____	En el código penal se tipifica: Art. 214. Estafa Art. 220 Manipulación de sistemas informáticos	- Puesto 11 ranking global de phishing	- Posición **97** en ranking global 2018 - Posición 1**4** en ranking regional 2018 - Nivel medio en ciberseguridad	- Computer Security Incident Response Team (CSIRT-Panamá-2011) - Estrategia Nacional de Seguridad Cibernética y

					Art- 224 daños Delitos contra la seguridad informática Art. 283 al Art. 286 Falsificación informática Art. 362 y 364		(0,369 puntaje IGC)	Protección de Infraestructuras Críticas (2013) - Proyecto de Ley 558 para modificar código penal (2017)
13. Paraguay	República presidencialista	Convenio de Budapest	Código Penal de Paraguay Uso de términos: datos informáticos	_____	En el código penal se tipifica: Art. 174 Alteración de datos Art. 175 Sabotaje de computadoras Art. 188 operaciones fraudulentas por computadoras Art. 248 alteración de datos Art. 249. Equiparación para el procesamiento de Datos Art. 253; 188;	- 372.945 ataques a redes en la última semana de enero 2020[79]	- Posición **66** en ranking global 2018 - Posición 5 en ranking regional 2018 - Nivel medio en ciberseguridad (0,603 puntaje IGC)	Unidad Especializada en Delitos Informáticos del Ministerio Público

[79] Ciberamenazas en tiempo real. Fuente: Kaspersky (26 de enero 01 de febrero 2020). https://cybermap.kaspersky.com/es/stats#country=124&type=wav&period=w

14. Perú	República presidencialista	Convenio COMJIB	Código Penal de Perú Artículo 207 derogado por cumplimiento de Ley 30096	Ley de Delitos Informáticos 30096 año 2013 (11 artículos en total) Uso de términos: Delitos informáticos	En la ley se tipifica: Art. 2 Acceso ilícito Art. 3 y 4 Atentado contra la integridad de datos y sistemas informáticos Art. 6 y 7 Delitos contra la intimidad y el secreto Art. Suplantación de identidad.	- 204.701 ataques web en la última semana de enero 2020[80]	- Posición **95** en ranking global 2018 - Posición 13 en ranking regional 2018 - Nivel medio en ciberseguridad (0,401 puntaje IGC)	División de Investigación de Alta Tecnología (Policía Nacional de Perú)
15. República Dominicana	República presidencialista	Convenio de Budapest (2008)	Código Penal (1984) última actualización 2019	Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología año 2007 (total 67 artículos) Uso de términos: delitos de alta tecnología (informático; cibernético, telecomunicaciones)	En la ley se tipifica: Art. 5 al 11 Disponibilidad de datos y sistemas de información (código de acceso, acceso ilícito, sabotaje) Art. 12 al 24 Delitos de Contenido Art. 26 Delitos de telecomunicaciones Art. 28 Actos de terrorismo	- 202.401 ataques a redes en la última semana de enero 2020[81]	- Posición **92** en ranking global 2018 - Posición 10 en ranking regional 2018 - Nivel medio en ciberseguridad (0,43 puntaje IGC)	- Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología - Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) - División de Investigaciones de Delitos Informático
16. Uruguay	República presidencialista	Convenio COMJIB	Código Penal Art. 277 bis Pornografía infantil	_____	_____	- 72.211 401 ataques a redes en la última semana de enero 2020	- Posición **51** en ranking global 2018 - Posición 3 en ranking regional 2018 - Nivel alto en	- Departamento de Delitos tecnológicos de la Jefatura de Policía de Montevideo - Centro Nacional de Respuesta a

[80] Ídem 7.
[81] Ídem 8.

							ciberseguridad (0,681 puntaje IGC)	Incidentes de Seguridad Informática - Proyecto de Ley 2016
17. Venezuela	República Fed. Presidencialista	_____	Código Penal última actualización 2000	Decreto con fuerza de ley sobre mensajes de datos y firmas electrónicas Ley Especial contra los Delitos Informáticos Ley 37.313 – año 2001 Uso de términos: Delitos informáticos	En la ley se tipifica: Art. 6 al 31 Art. 6 al 12. Delitos contra los Sistemas que Utilizan Tecnologías de Información (espionaje informático) Art.20 al 22 Contra la Privacidad	- 70.4% de vulnerabilidad - Puesto 2 ranking global de phishing	- Posición **99** en ranking global 2018 - Posición 16 en ranking regional 2018 - Nivel bajo en ciberseguridad (0,206 puntaje IGC)	- Cuerpo de Investigaciones Científicas, Penales y Criminalísticas

Fuente: Gamba, Jacopo. 2010. Panorama del derecho informático en América Latina y el Caribe, CEPAL; Ciberseguridad ¿estamos preparados en América Latina y el Caribe? Informe de ciberseguridad 2016; Kaspersky amenazas en tiempo real: https://cybermap.kaspersky.com/es; Índice de Ciberseguridad Global 2018. https://www2.deloitte.com
Elaborado por: Autoría propia.

Anexo 2: Ecuador: Indicadores de Medición del índice de ciberseguridad de la OEA

Dimensiones	Niveles de madurez de capacidad en ciberseguridad
Política y estrategia	—
Estrategia nacional de seguridad cibernética oficial o documentada	Inicial: No hay evidencia de la existencia de una estrategia nacional de seguridad cibernética; si existe un componente cibernético, puede ser responsabilidad de uno o más departamentos del gobierno
Defensa cibernética	En cuanto a organización, su indicador mantiene un estado formativo, evidenciando que la defensa cibernética se incorpora a las diferentes ramas de las fuerzas armadas, pero no existe una estructura central de mando y control.
Cultura y sociedad	— —
Mentalidad de seguridad cibernética	Solamente en el sector privado se mantiene un nivel de madurez formativo, que han comenzado a darle prioridad a la seguridad cibernética
Conciencia de seguridad cibernética	Formativo: Empresas líderes han comenzado a darle prioridad a una mentalidad de seguridad cibernética mediante la identificación de prácticas de alto riesgo.
Confianza en el uso de Internet	Formativo: La confianza en los servicios en línea se identifica como una preocupación; los operadores de infraestructuras toman en consideración medidas para fomentar la confianza en los servicios en línea; sin embargo, no se han establecido medidas.
Privacidad en línea	Inicial: La discusión con grupos de interés sobre asuntos de privacidad ha comenzado a nivel gubernamental.
Educación	— —
Disponibilidad nacional de la educación y formación cibernéticas	Formativo: existe mercado para la educación y la formación en seguridad de la información, así como dirigidas a profesionales para incrementar el atractivo de las carreras en ciberseguridad.
Desarrollo nacional de la educación de seguridad cibernética	Formativo: Existen incentivos para la formación y la educación
Formación e iniciativas educativas públicas y privadas	Formativo: No hay transferencia de conocimientos por parte de los empleados de seguridad cibernética capacitados; debido a una formación limitada, solo hay uso informal de herramientas, modelos o plantillas

Gobernanza corporativa, conocimiento y normas	Formativo: Las juntas directivas tienen algún conocimiento de cuestiones de seguridad cibernética, pero no de la forma en que estas podrían afectar a la organización,
Marcos legales	—
Marcos jurídicos de seguridad cibernética	Formativo: Los socios experimentados han sido consultados para apoyar el establecimiento de marcos jurídicos y reglamentarios; se han identificado prioridades clave para la creación de marcos legales de seguridad cibernética pero aún no se han establecido.
Investigación jurídica	Formativo: Existe una capacidad mínima de investigación para indagar delitos que involucren pruebas electrónicas,
Divulgación responsable de la información	Inicial: No se reconoce la necesidad de una política de divulgación responsable en las organizaciones del sector público y privado.
Tecnologías	—
Organizaciones de coordinación de seguridad cibernética	Formativo: La función de mando y control está en manos, de manera informal, del mismo modo existe un equipo o personal de respuesta a incidentes en el país, con roles y responsabilidades identificadas.
Respuesta a incidentes	Formativo: en cuanto a coordinación, se han identificado y publicitado directores de incidentes en cada agencia y ministerio a nivel nacional; pero los canales de comunicación entre estos directores siguen siendo ad hoc e incoherentes.
Protección de la Infraestructura Crítica Nacional (ICN)	Inicial: en todos sus indicadores marcan el estado inicial, pero el que destaca es la de coordinación donde se destaca que hay poca o ninguna interacción entre los ministerios gubernamentales y los propietarios de los activos críticos. .
Gestión de crisis	Inicial: No hay entendimiento, o es mínimo, de que la gestión de crisis es necesaria para la seguridad nacional;
Mercado de la ciberseguridad	Inicial: Poca o ninguna tecnología se produce en el país; pueden estar restringidas las ofertas internacionales o son vendidas con un sobreprecio, tampoco se ha identificado la necesidad de un mercado de seguros ante delitos informáticos.

Fuente: Ciberseguridad ¿estamos preparados en América Latina y el Caribe? Informe de ciberseguridad 2016.
Elaborado por: Autoría propia.

Anexo 3: Reseña cronológica 2006-2014 del caso Julian Assange[82]

2006-2007. Fundación WikiLeaks. Organización sin fines de lucro que abre un sitio web para evidenciar, divulgar y filtrar información sensible de varios países.

7 Noviembre 2007. Divulgación del Manual de procedimiento militar en el campamento Guantánamo.

5 Abril 2010. Publicación de video de muerte a 11 iraquíes por soldados estadounidenses.

25 Julio 2010. Publicación de alrededor de noventa mil documentos de reportes de la guerra de Afganistán.

Agosto 2010. Se abre una investigación contra Assange por acoso sexual en Suecia y noviembre del mismo año se emite una orden de arresto.

Octubre 2010. Publicación de trescientos noventa mil documentos clasificados del Pentágono relacionados a ataques en Irak.

28 Noviembre 2010. Publicación de doscientos cincuenta mil documentos que revelaron la disposición de que diplomáticos estadounidenses hagan espionaje a políticos extranjeros y altos funcionarios de la ONU.

Diciembre 2010. WikiLeaks.org fue dado de baja del sistema y entregado al Partido Pirata helvético y PayPal canceló su cuenta.

7 Diciembre 2010. Fue detenido por autoridades británicas por orden de la justicia sueca por los cargos de acoso sexual y violación. Después de diez días fue liberado con derecho a una fianza.

S/f 2010. Un tribunal secreto estadounidense presenta cargos contra Assange de manera confidencial.

7 Febrero 2011. Inicio de proceso de extradición de Assange a Suecia y en noviembre del mismo año el Tribunal Supremo de Londres aprueba su extradición.

Octubre 2011. Assange declara que no publicará más secretos de Estado, debido a la falta de financiación.

[82] Para esta primera parte de la cronología me he remitido a los acontecimientos descritos por el trabajo investigativo de Marta Forn Bosch (2015) de la Universitat Abat Oliba CEU.

17 Abril 2012. Assange entrevista al ex presidente de Ecuador, Rafael Correa. Días más tarde, éste revela que Assange está siendo perseguido por los propios medios de comunicación por filtrar información de Estados Unidos.

14 Junio 2012. El Tribunal Supremo de Inglaterra rechaza la petición de Assange para que su caso sea reabierto y así evitar su extradición a Suecia.

19 Junio 2012. Assange se refugia en la Embajada de Ecuador en Londres y pide asilo político para evitar su extradición. Al día siguiente la policía advierte a Assange que violó el arresto domiciliario y puede ir a prisión.

5 Julio de 2012. Wikileaks empezó a publicar más de dos millones de correos electrónicos de importantes personajes políticos relacionados con el régimen Sirio.

3 Agosto de 2012. Ante el declive de otorgar un salvoconducto a Assange para salir de Londres, el juez Baltasar Garzón, abogado de Assange, calificó este hecho como algo antijurídico.

15 y 16 Aagosto 2012. Autoridades de Gran Bretaña amenazan con entrar a la Embajada de Ecuador, si Assange no se entrega a la justicia británica. Posteriormente, Ecuador confirma el asilo político al informático australiano, asumiendo que este correría peligro por ser sujeto de interés contra Estados Unidos.

2013 Inicio de negociaciones

17 de Junio. Acuerdo entre ex canciller ecuatorianos Ricardo Patiño y el canciller británico Williann Hague, para crear una comisión que solucione el caso Assange.

26 Noviembre. Estados Unidos anuncia que no presentará cargos contra Assange.

Reseña cronológica 2014-2019

Esta segunda parte de la cronología recopila información de diferentes periódicos digitales que ayudaron a dar cuenta de una fase de cambios en la diplomacia internacional, evidenciando las reglas de juego ocultas en los primeros años de asilo político de Julian Assange.

Estado de salud crítico

*7 Junio 2014***.** Mediante declaración jurada de Assange**,** afirman presunciones de que Estados Unidos tiene planes de enjuiciarlo bajo la Ley de espionaje o terrorismo.

Agosto 2014. Assange afirma su intención de abandonar la Embajada, aduciendo que su estado de salud se encuentra crítico.

5 Febrero 2016.[83] Tras la arbitrariedad de Suecia y Reino Unido, la ONU solicita una indemnización y la liberación de Assange.

Julio 2016. WikiLeaks revela alrededor de veinte mil correos electrónicos de la entonces candidata presidencial Hillary Clinton, desprestigiando seriamente su campaña electoral. Según analistas políticos esta estrategia habría llevado a Donald Trump a la presidencia de Estados Unidos.

Octubre 2016. Luego de que se publicaran correos de Hilary Clinton, el gobierno del exmandatario Rafael Correa, solicita a Assange que no intervenga en asuntos políticos y ordena retirar el internet a servicio del informático.

19 Mayo 2017. Se declara el cierre de los motivos de investigación en contra de Assange, la misma que se inició en el 2010 por la Fiscalía Sueca.

24 Mayo 2017. Lenin Moreno asume la presidencia del Ecuador hasta el 2021, después de que Rafael Correa finalizara su periodo presidencial.

26 Agosto 2017. El independentismo catalán es apoyado por Assange, según miles de twits publicados por el mismo.

31 Julio 2017. A días de la segunda vuelta de las elecciones presidenciales en Francia, la página web Wikileaks filtra miles de correos de Emanuel Macron.

12 Diciembre 2017. El gobierno ecuatoriano otorga la nacionalidad a Assange como recurso de protección que le permita asumir un cargo diplomático y así poder salir de Reino Unido, la cual no fue aceptada por este país.

17 Diciembre 2017. Assange es amenazado por Lenin Moreno, para que no intervenga en la crisis de Cataluña.

s/f 2017 Mike Pompeo (ex director de la CIA), ministro de Exteriores de Estados Unidos, denomina a WikiLeaks como "agencia de inteligencia enemiga no estatal".[84]

24 Enero 2018. Según declaraciones de Lenin Moreno, Assange es un problema para su gobierno.

28 Marzo 2018. Assange es privado de toda conexión a internet, porque el gobierno ecuatoriano considera que los pronunciamientos de Assange refiriéndose a la política de otros países, los compromete.

---

[83] https://www.dw.com/es/cronolog%C3%ADa-del-caso-assange/a-46723957

[84] Declaración obtenida en periódico digital France 24. https://www.france24.com/es/20200223-cinco-claves-caso-julian-assange-extradicion-estados-unidos

17 Mayo 2018. La seguridad especial que mantenía vigilado a Assange en la Embajada de Ecuador en Londres, es retirada por el gobierno ecuatoriano.

Terminación forzada de asilo[85]

Enero 2019. WikiLeaks publica documentación confidencial del Vaticano.

Abril 2019. Estados Unidos a través de su Departamento de Justicia acusa a Assange por delitos informáticos contra el Estado, cuya pena es de cinco años en prisión.

11 Abril 2019. Assange es detenido por las autoridades británicas, luego de que el presidente ecuatoriano Lenin Moreno retirara el asilo político. El momento de su detención se realizó de manera forzada, sacándolo de la Embajada ecuatoriana.

La policía británica afirmó que su detención se debió al incumplimiento de presentación ante los tribunales del Reino Unidos en 2012.

Posteriormente el Ministerio del Interior corroboró la existencia de la solicitud de extradición por parte de Estados Unidos.

16 Abril 2019. Autoridades británicas lo mantienen bajo su custodia hasta el dictamen de su sentencia, cuya condenan sería de 12 meses de prisión por incumplimiento de su libertad condicional.

Mayo 2019. La justicia de Estados Unidos formula un total de 18 cargos, incluyendo la violación de la Ley de espionaje. La pena puede llegar hasta los ciento setenta y cinco años de cárcel.

[85] Información obtenida del portal de la BBC News. https://www.bbc.com/mundo/noticias-internacional-47897043

Anexo 4: Reseña cronológica del Caso Ola Bini

Febrero 2013. Llega a Ecuador con fines de trabajo por la compañía de tecnología ThoughtWorks para brindar un taller sobre temas de seguridad informática para la SENESCYT.

Noviembre 2013. Regresó a Quito para domiciliarse en el país, tras anteriores viajes de trabajo.

Año 2015. Ola Bini realiza un informe de seguridad informática en Ecuador y encuentra la existencia de un sistema viejo denominado TELNET, que posee fallas de seguridad y que son utilizados por servidores de instituciones públicas y privadas, entre ellas la Corporación Nacional de Telecomunicaciones (CNT). Esta información es trasmitida a su colega Marco Argüello, programador ecuatoriano, quien tenía una relación contractual con CNT para identificar vulnerabilidades en el sistema.

11 Abril 2019. Durante este día se han identificado diferentes eventos que llevaron a la detención arbitraria de Ola Bini:

- 04:27 (Hora Ecuador). El gobierno de Lenin Moreno retira el asilo político a Julian Assange, inmediatamente la Embajada de Ecuador en Londres entrega a Assange a las autoridades británicas.
- En rueda de prensa María Paula Romo, Ministra del Interior, declaró que podrían haber ataques informáticos a los sistemas gubernamentales, tras la detención de Assange y que por consecuencia sus aliados en Ecuador deberían ser investigados.[86] Según el parte policial es "una de las personas que la Ministra del Interior nombró ante los medios de comunicación como un hacker ruso y/o suizo, miembro de Wikileaks".[87]
- 15:19 Ola Bini es detenido en el aeropuerto Mariscal Sucre por la Unidad de Investigación de Delitos Tecnológicos perteneciente a la Policía Nacional, durante su salida a Japón. Fue llevado a una oficina de la INTERPOL dentro del Aeropuerto.[88] Le presentaron una orden de arresto que no era dirigida al señor Bini sino a un viajero ruso.
- 22:04. Se emitió una orden de allanamiento domiciliario, donde confiscaron dispositivos tecnológicos (unidades USB, ordenadores, libros).

[86] La República. https://www.larepublica.ec/blog/politica/2019/07/05/ola-bini-acude-a-la-fiscalia-a-dias-del-fin-de-la-instruccion-fiscal/

[87] GK Studio. https://gk.city/2019/09/02/defensa-ola-bini-denuncio-irregularidades/

[88] Declaraciones emitidas en la entrevista realizada por el canal digital La Posta (24 junio 2019). https://www.youtube.com/watch?v=z1MEgQRhvSc

12 Abril 2019. Se informa al abogado de Ola Bini que será transferido a la Unidad de Flagrancia. Horas más tarde logra reunirse con su abogado en una reunión privada con la ayuda del consulado sueco.

En la audiencia de formulación de cargos se dictamina que su arresto y detención no eran ilegales y que debía ser llevado a prisión preventiva debido que existían motivos suficientes para iniciar una investigación en su contra. Se ordenó que sus activos fueran congelados. Su acusación se basó en evidencia relacionada con los gastos en servicios de internet y el material allanado.

20 Junio 2019. La Corte Provincial de Pichincha lo declaró en libertad, aceptando el recurso de habeas corpus, como solicitud presentada por su defensa, retirando la prisión preventiva. Entre las medidas cautelares debe presentarse cada viernes ante la sede fiscal pendiente del caso.

26 Agosto 2019. Aministía Internacional denuncia que el gobierno ecuatoriano está interviniendo políticamente en el proceso judicial.[89]

29 Agosto 2019. Audiencia de reformulación de cargos contra Bini por el delito de acceso no consentido a un sistema informático. Antes fue acusado de ataque a la integridad de sistemas informáticos. Además se presentan pruebas de que había visitado catorce veces a Assange, según autoridades ecuatorianas.[90]

Representantes de CNT y el fiscal del caso declararon que Bini había ingresado sin ninguna autorización a las redes privadas de Petroecuador y de la Secretaría Nacional de Inteligencia (SENAIN).

31 Agosto 2019. Finaliza la instrucción fiscal.

2 Septiembre 2019. Ola Bini solicita acceder a su expediente completo, luego de que haya finalizado su instrucción fiscal.[91]

5 Septiembre 2019. Allanamiento domiciliario de Fabián Hurtado, un perito informático contratado por la defensa de Ola Bini por presunciones de fraude procesal, al

[89] Ecuavisa (27 agosto 2019). https://www.ecuavisa.com/articulo/noticias/politica/522776-fiscalia-solicita-cambio-delito-contra-ola-bini

[90] Según declaraciones de Ola Bini al periódico El Comercio, la reformulación de cargos se hizo dos días que acabara la instrucción fiscal, "No tuvimos los 30 días preceptivos constitucionales para preparar la defensa". https://www.elcomercio.com/actualidad/ola-bini-fiscalia-juicio-ciberseguridad.html

[91] La República (2 de septiembre de 2019). https://www.larepublica.ec/blog/politica/2019/09/02/ola-bini-exige-acceso-expediente-completo/

entregar información engañosa en su hoja de vida. Antes había participado como perito en el caso del ex presidente Jorge Glas.[92]

25 Septiembre 2019. Lenin Moreno en una entrevista con CNN anuncia que Ola Bini ha intervenido en la política de Ecuador y de otros países.

9 Enero 2020. El abogado de Ola Bini, publica mediante fotos y videos en las redes sociales, que supuestamente estaba siendo vigilada la casa de Bini por presuntos policías[93]

17 Marzo 2020. Fijación de la fecha para su juzgamiento.

11 Mayo 2020. En razón de la pandemia mundial COVID-19, de acuerdo a las disposiciones del Comité de Operaciones de Emergencia (COE), la Corte Nacional resuelve suspender toda tramitación normal de causas no flagrantes y por tanto el juicio de Ola Bini, ha sido suspendido hasta nuevo aviso.

[92] GK Studio (2 de septiembre de 2019). https://gk.city/2019/09/09/allanaron-casa-perito-fabian-hurtado/

[93] Aministía Internacional (3 de marzo de 2020). https://www.amnesty.org/es/latest/news/2020/03/ecuador-authorities-must-monitor-trial-digital-defender-ola-bini/

Anexo 5: Reseña cronológica robos de datos personales la población ecuatoriana[94]

Enero 2019 (fecha aproximada). La base de datos fue expuesta públicamente.

6 Septiembre 2019. Noam Roten y Ran Locar, informáticos israelíes que trabajan para la empresa vpnMentor, encontraron fallas en un sistema de seguridad, y encontraron un servidor con información personal de casi diecisiete millones de ecuatorianos. Este sistema era administrado por una empresa ecuatoriana de Marketing conocida como Novaestrat.

15 Septiembre 2019. Se cerró el acceso a la base de datos.[95]

16 Septiembre 2019. El gobierno ecuatoriano difundió esta información públicamente, anunciando las acciones para bloquear al servidor que alojaba la información y que iniciará un proceso investigativo contra los posibles implicados.

Se inician investigación contra la empresa Novaestrat y se detiene a su representante legal William Roberto G.M.

17 Septiembre 2019. Funcionarios de Novaestrat son liberados.

18 de Septiembre 2019. En declaraciones en medios de comunicación,[96] Andrés Michelena, Ministro de Telecomunicaciones indica que solo el 26% de las instituciones públicas guardan su información sensible en sitios seguros.

24 Septiembre 2019. Ran Locar publica en su cuenta de twiter que bases de datos de instituciones públicas y de información de ecuatorianos han sido expuestos en un servidor de Miami. Indica que esta información ha estado disponible desde enero 2019 y que se presume que todos los datos son públicos y que cualquiera podría acceder a ellos.

25 Septiembre 2019[97]. Nueva vulneración de información sensible es denunciada por los informáticos isralíes. Esta base de datos incluía los montos de seguros privados, sueldos del mes de agosto y otro tipo de información reservada. En este caso otra empresa de ciberseguridad ecuatoriana se encuentra asociada a la protección de esta información.

---

[94] El Comercio (24 septiembre 2019). https://www.elcomercio.com/actualidad/venta-datos-ecuatorianos-investigadores-informatica.html

[95] Ola Bini. "Análisis de la filtración de Novaestrat". https://autonomia.digital/es/privacy/2019/09/28/analysis-novaestrat.html

[96] Entrevista Rafael Bonifaz, experto en seguridad informática (18 septiembre 2019). http://www.pichinchauniversal.com.ec/experto-en-seguridad-informatica-migrar-datos-a-servidores-de-cnt-no-es-la-solucion/

[97] El Telégrafo (25 septiembre 2019). https://www.eltelegrafo.com.ec/noticias/politica/3/gobierno-denuncia-robo-datos