PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE DERECHO

Análisis de la política criminal peruana frente a la cibercriminalidad pura

Tesis para obtener el título de Abogado que presenta el bachiller:

Luis Ricardo Llanos Carrera

Asesor:

Julio Alberto Rodríguez Vásquez

Lima, 2022

PUCP
Sistema de Bibliotecas

INFORME DE SIMILITUD

Yo, **JULIO ALBERTO RODRIGUEZ VÁSQUEZ**, docente de la Facultad de **DERECHO** de la Pontificia Universidad Católica del Perú, asesor(a) de la tesis/el trabajo de investigación titulado:

Análisis de la política criminal peruana frente a la cibercriminalidad pura.

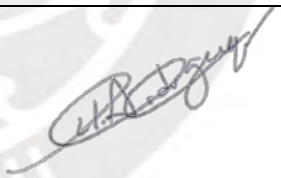
del/de la autor(a)/ de los(as) autores(as)

LUIS RICARDO LLANOS CARRERA

dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 29%. Así lo consigna el reporte de similitud emitido por el software *Turnitin* el 28/04/2023
- He revisado con detalle dicho reporte y confirmo que cada una de las coincidencias detectadas no constituyen plagio alguno.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lugar y fecha: **Lima, 28 de abril de 2023**

Apellidos y nombres del asesor / de la asesora: **RODRIGUEZ VÁSQUEZ, JULIO ALBERTO**	
DNI: 70240434	
ORCID: https://orcid.org/0000-0002-8754-4611	

Resumen

La presente investigación analiza la política criminal peruana vigente que combate y previene el fenómeno de la cibercriminalidad en la vertiente pura. Entiéndase esta por aquella actividad cibercriminal que, valiéndose del desarrollo y uso de las TIC, dirige ciberataques hacia computadoras, programas informáticos (*software*), redes, terminales, y cualquier operatividad tecnológica basada en la comunicación digital de contenidos, que no tenga una réplica en términos de referencia fuera del ciberespacio, de ilícitos que se realizaban de otro modo, en el espacio físico. La finalidad de la investigación es identificar si la normativa desplegada por el Estado de los últimos años en materia de delitos informáticos, ha dotado a la política criminal de un enfoque integral y pluridimensional que posibilite comprender y atender adecuadamente los desafíos de la cibercriminalidad pura.

Palabras clave: cibercriminalidad pura, política criminal, enfoques de prevención del delito, estrategias de prevención del delito, ciber-criminología, delito informático.

Abstract

The present investigation seeks to analyze the current Peruvian criminal policy enabled in place to mitigate and prevent cyber criminality offenses related to cyber-dependent crimes. This is understood as that cybercriminal activity that, using the development and use of ICT, directs cyberattacks towards computers, computer programs (software), networks, terminals, and any technological operation based on digital communication of content, which does not have a replica in terms of reference outside of cyberspace, of crimes that were already being carried out, otherwise, in physical space. The purpose of the research is to identify whether the regulations deployed by the State in recent decades have provided criminal policy with a comprehensive and multidirectional approach that makes it possible to understand and adequately address the challenges of cyber-dependent crimes.

Keywords: cyber-dependent crimes, criminal policy, crime prevention approaches, crime prevention strategies, cyber-criminology, computer crime.

Índice de contenido

Introducción

El problema general de la proliferación del fenómeno cibercriminal puro, es que con frecuencia permanece encubierto dentro de una cifra negra, la cual no ha sido plenamente identificada como dicho delito en las estadísticas proporcionadas por el Ministerio Público a finales del año 2019. El objetivo del trabajo analiza la política cibercriminal nacional y los enfoques de prevención del delito, o estrategias político-criminales utilizadas hacia fines del año 2020 para combatir, prevenir, y mitigar el fenómeno de la cibercriminalidad pura.

El concepto de cibercriminalidad pura abarca la actividad cibercriminal situada exclusivamente dentro del ciberespacio, constituyéndose este último ámbito en la única vía posible para cometer el delito y alcanzar el objetivo criminal, a diferencia de otras vertientes cibercriminales que pueden cometerse en la intersección del ciberespacio, y la realidad física. De acuerdo con la información divulgada por el Ministerio Público a finales del año 2019, se registró un incremento en el total de delitos informáticos en un 99.74% en relación con el total de delitos cometidos el año previo 2018.

Es así que a partir de esta realidad criminológica nace la necesidad de plantearse la presente problemática, con la finalidad de explicar en base a los estudios criminológicos más recientes, la modalidad de cibercriminalidad pura, e identificar y caracterizar las medidas político-criminales vigentes implementadas por el estado, a nivel nacional, para prevenirla. La metodología empleada es de tipo dogmática y bibliográfica, en la medida que es necesario adentrarse en las fuentes del derecho nacional e internacional, además de examinar y seleccionar conceptos con el objetivo de alcanzar un conocimiento sistematizado, a fin de aproximarse a la política cibercriminal nacional de manera exhaustiva, cuyo desarrollo normativo en torno a los delitos informáticos se extiende a lo largo de las últimas tres décadas.

El primer capítulo desarrollará el concepto de cibercriminalidad pura, así como la noción de cibercrimen entendido bajo interpretaciones amplias y restrictivas, y las vertientes de tipo replica y, de contenido. Dentro de la cibercriminalidad pura se establecerá los delitos que la conforman como son; la intrusión informática -*hacking*-, la propagación de virus -*malware*-, y los ataques de denegación de servicios y conexos -*DoS/DDoS*-. Asimismo, se indicará porque la vertiente cibercriminal pura con frecuencia se origina en ecosistemas cibercriminales altamente especializados que respaldan toda la cadena de valor del cibercrimen, además de impulsar la economía digital subterránea.

Se indicará que el concepto de política criminal empleado para este trabajo se refiere aquella que bajo la cual toda acción estatal se encuentra enmarcada en el modelo de Estado Constitucional de Derecho, y es conducente a resolver el problema de la criminalidad a través de la prevención del delito. En esta línea se explicarán los enfoques de prevención de delito de corte primario, secundario, y terciario, así como las estrategias de prevención del delito que pueden ser de tipo situacional, del desarrollo, y comunitario.

Dentro de este capítulo se identificará cuatro propuestas de prevención utilizadas en la actualidad para combatir el fenómeno de la cibercriminalidad pura y demás vertientes. Estas son: Auto-Regulación y Co-Regulación de Asociaciones Público-Privadas de Tropina y Callanan (2015), Privatización de la Ciberseguridad de Sales (2018), Monitoreo Preventivo del Cibercrimen de Dupont (2019), y El Daño Extracontractual de la Habilitación Negligente del Ciberdelito de Rustad y Koening (2005).

El segundo capítulo ahondará en una aproximación criminológica de la cibercriminalidad pura, a través de estudios empíricos realizados por tres grupos de teorías criminológicas, no sin antes explicar que para entender las operatividades de las teorías criminológicas es necesario adoptar una explicación multifactorial del fenómeno cibercriminal, en la medida que ninguna de las teorías propuestas permite explicarlo a partir de una causa única, sino de un "paquete" de condiciones interrelacionadas de aplicabilidad variable.

Por lo tanto, para entender el fenómeno cibercriminal puro se emplearán tres conjuntos de teorías criminológicas, el primero se refiere a las llamadas teorías de control; dentro de ellas, se sitúa la teoría del autocontrol, la de los vínculos sociales, y la deriva digital. El segundo grupo de teorías son las llamadas teorías culturales; que incluye a la teoría del aprendizaje social, la desconexión moral, y las subculturas. El tercer grupo de teorías se refiere a las teorías de la oportunidad; que incluye a la teoría de las actividades rutinarias, y las técnicas de prevención situacional.

El tercer capítulo explorará las experiencias comparadas en torno a la prevención, y lucha contra la cibercriminalidad de siete países, y la Unión Europea, quienes ostentan un notable protagonismo internacional en el ámbito de políticas de ciberseguridad. Como se verá en el análisis de los países bajo estudio, se revelará que en todas las regiones se presentan contextos de ciberseguridad distintos, donde las ventajas de algunos países no las comparte el resto de estados. Estas diferencias obedecen a razones de

diversa índole, como de naturaleza presupuestal, de política criminal, de políticas de prevención, entre otros factores. En este sentido se indicará porque luego de analizar la experiencia comparada de estos Estados en torno a la prevención y persecución de la actividad cibercriminal, es necesario contar con un marco legal adecuado para que los Estados apliquen normativas pertinentes que posibiliten combatir de manera eficiente la cibercriminalidad. Caso contrario, no sería posible combatir la ciberdelincuencia en igualdad de armas con otros agentes estatales, si existe un grupo de ellos que no cuenta con el conocimiento empírico y la experiencia acumulada en dichos entornos regulatorios y/o normativos.

Finalmente, el cuarto capítulo presentará las tres décadas de desarrollos normativos de la política cibercriminal nacional, resumiendo los hitos alcanzados en tablas según criterios clasificatorios como: norma, fecha de publicación, medidas político-criminales incluidas, y su especificidad en relación a la cibercriminalidad pura. En esta línea se revelará que después de comparar un total de cuarenta medidas para combatir y/o prevenir la cibercriminalidad implementadas desde la década de los noventa hasta la actualidad, se identificó un subgrupo de seis que tienen incidencia directa en la cibercriminalidad pura.

Cuatro de estas medidas fueron subsumidas dentro de la prevención secundaria del delito, siendo estas; a) Ley 27309 que incorporó los delitos informáticos al Código Penal (2000), b) Ley 30096 - Ley de delitos informáticos (2013), c) Ley N°30999 - Ley de Ciberdefensa (2019) y d) la Resolución legislativa N°30913 - que aprobó la adhesión a la Convención de Budapest (2019). Mientras que las dos restantes se subsumieron dentro de las estrategias de prevención situacional de delito, siendo estas: e) la Resolución Ministerial 360-2009 que creó el Pe-CERT, y f) la creación de la fiscalía especializada en ciberdelincuencia del MPFN con competencia nacional.

Sin embargo, se evidenciará que en la actualidad no existe una política cibercriminal integral que combata y prevenga el fenómeno de la cibercriminalidad pura. Ni tampoco existe evidencia consistente que revele como han funcionado los marcos legales vinculados a la cibercriminalidad pura en las últimas tres décadas. A modo de cierre, se explicará porque la implementación de una futura política cibercriminal debe contemplar necesariamente la adopción de un enfoque preventivo del delito entendido de manera holística, y pluridireccional que facilite la implementación de estrategias de prevención situacional, del desarrollo, y comunitario, así como de enfoques ademas de la prevención secundaria de tipo primario, y terciario.

CAPÍTULO 1

Marco conceptual: Cibercriminalidad pura y Política Criminal

1. Cibercrimen

1.1 Concepto de cibercrimen

Los delitos informáticos ocurren en el ciberespacio y constituyen ilícitos que emplean las redes y la tecnología para causar daño. El cibercrimen es un fenómeno delictivo que se encuentra en pleno crecimiento, esto se debe al avance tecnológico producido por la conectividad global contemporánea.

De acuerdo con Chawki, Darwish y Tyagi cualquier actividad delictiva que involucre una computadora como instrumento, objetivo o medio para perpetuar más delitos, entra en el ámbito del cibercrimen (Chawki et al., 2015).

A pesar de lo antes dicho, el termino delito informático ha sido reemplazado últimamente por el de cibercrimen. Sobre este concepto, Miró señala que "proviene del término anglosajón *cybercrime*, el cual resulta producto de la unión del prefijo *cyber*, derivado del término *cyberspace*, y el término *crime*" (2011, p.2). Además, el criminólogo español señala que esta categoría abarca la ciberdelincuencia vinculada al uso de las Tecnologías de la Información y la Comunicación - en adelante TIC.

Sobre el dominio de este término, Miró señala que los estudios criminológicos y de vertiente jurídica procedente de países anglosajones habrían impuesto el mencionado término, en vez de otros que podrían compartir similares significados como "*virtual, online, high-tech, digital, computer-related, internet-related, electronic*, y *e-crimes*" (2011, p. 5).

Por el contrario, el concepto de cibercriminalidad supone una categoría criminológica que no tiene sentido normativo (2013). Dicho esto, cuando se emplea el término "cibercrímenes" se hace referencia a conductas especificas situadas o subsumidas dentro del fenómeno de la cibercriminalidad.

Es así como, bajo una interpretación amplia de "cibercrimen", esta incluiría cualquier comportamiento delictivo realizado en el ciberespacio que no podría haberse dado fuera de él. No obstante, bajo una interpretación restrictiva, se necesitaría de distintos criterios para seleccionar o abarcar a algunas conductas realizadas en el ciberespacio.

Sobre este punto, Miró señala que por un lado el acoso sexual mediante internet sería considerado bajo una interpretación amplia como un cibercrimen, sin embargo, este mismo delito no sería considerado como tal bajo una concepción restringida por tener su referente fuera del ciberespacio.

Por otro lado, un delito de "denegación de servicios" clasificaría como cibercrimen bajo la interpretación amplia y restrictiva, porque la realización de dicha conducta solo es posible vía el ciberespacio, concretamente por medio de internet (2013).

1.2 Tipología del cibercrimen

Con respecto a las tipologías de los cibercrímenes en el ciberespacio, como se dijo, las modalidades pueden clasificarse según diversos criterios planteados por el autor. Es así que de acuerdo a la literatura especializada la clasificación de los cibercrímenes son los siguientes:

Tabla 1
Tipología de cibercriminalidad según la literatura especializada

Fuente	**Tipo de cibercrimen**	**Definición**
Abernathy y McMillan, 2018, p.72	La computadora como objetivo del delito	Supuestos de *hacking*, virus informáticos, ataques de denegación de servicio, y *malware o* código malicioso, se requiere de conocimiento técnico de los autores.
	La computadora como herramienta del delito	El individuo es el objetivo principal del delito y la computadora es solo la herramienta para facilitarlo. requiere menos experiencia técnica. Ej. estafa, fraude, robo de identidad, desinformación, *phishing* y *spam*.
	La computadora como componente incidental para la comisión de otros delitos	El uso de la computadora se convierte en delito cuando se emplea para mantener registros de actividades delictivas. Ej. pornografía infantil, lavado de dinero, atraer víctimas a situaciones comprometedoras y emprendimiento criminal.
	Los delitos asociados por la prevalencia de las computadoras	Ocurren debido a que los ordenadores son herramientas de uso obligatorio en la actualidad. Este tipo de delito ocurre solo porque existen computadoras. La piratería de *software* es un ejemplo de este tipo de delito.
	Ciber-intrusión	Mayormente a espacios donde hay derechos de autor y propiedad privada causando daños y perdidas como pueden ser la piratería y la distribución de virus.

Yar y Steinmetz, 2019, p. 137	Ciber-engaños y robos	Se refieren a aquellas infracciones relacionadas mayormente al ámbito financiero y patrimonial de entidades y personas.
	Ciber-pornografía	Son los Ilícitos relacionado a temas de indemnidad sexual y afines.
	Ciber-violencia	Esta modalidad puede abarcar infracciones de tipo discurso de odio, acoso y formas de violencia social y política.
	Cibercrimen contra el estado	Esta modalidad aglutinaría atentados que menoscaban leyes que protegen infraestructura estatal, como ataques terroristas, espionaje internacional y divulgación de secretos oficiales.
McGuire y Dowling, 2013, p. 5	Crímenes posibilitados por la tecnología *-cyber enabled crimes-*	Se tratarían de conductas tipificadas pero facilitadas por el uso de computadoras. Según los autores la gama de delitos posibilitados por la tecnología sería infinita, e incluiría desde delitos de cuello blanco, como transacciones financieras fraudulentas, robo de identidad y robo de información electrónica con fines comerciales, hasta tráfico de drogas, actividades voyeristas aberrantes, acoso, intimidación, chantaje, entre otras conductas desviadas.
	Crímenes dependientes de la tecnología *-cyber dependent crimes-*	Serían aquellos que no pueden existir fuera de la tecnología o sin el uso de esta. Ej. un cibercriminal que se propusiera infligir daños económicos a una empresa, aquella finalidad estaría mejor servida mediante el despliegue de robustos ataques informáticos, en vez de arrojar un molotov a la puerta principal del edificio.
Gordon y Ford, 2013, p. 5	Cibercrimen tipo I	Esta tipología incluye eventos singulares y discretos desde la perspectiva de la víctima y se relaciona mayormente con la utilización de *crimeware,* que es una clase de *malware* diseñado específicamente para automatizar el cibercrimen, como registradores de pulsaciones de teclas, virus, *rootkits* o *troyans.*
	Cibercrimen tipo II	Esta tipología incluye varios eventos repetidos desde la perspectiva de la víctima y facilitados por programas que no encajan en la utilización de *crimeware*, como el acoso, el chantaje, la manipulación de índices del mercado de valores, el espionaje corporativo, y actividades terroristas.
Kshetri, 2012, p. 6.	Cibercrímenes predatorios con fines de lucro *-Predatory cybercrimes for profit-*	Estos serían los actos que buscan dañar a la persona o a su propiedad, ej. robo financieros, o infracciones de propiedad intelectual, entre otros.
	Cibercrímenes basados en el mercado *-Market based cybercrimes-*	A diferencia de los primeros que podrían encajar en supuestos de redistribución de riqueza, esta segunda categoría si afectaría el balance del producto bruto interno, en la medida que al ofertarse nuevos bienes y servicios se estaría generando nuevos ingresos. ej. mercados de *software* ilegal, virus, cibercrimen como servicio, drogas, etc.

Miró, 2012, p. 50.	Ciberataque puro	Un cibercrimen puro es aquella conducta que solo será posible denominarla como tal si no puede disociarse de su pertenencia al ciberespacio. "El ilícito se asocia a una modalidad o categoría delictiva dentro de la cibercriminalidad caracterizada por ocurrir únicamente en el ciberespacio" (2011, p. 4). Ej. *Hacking*, propagación de virus e infecciones de *malware*, ataques *DoS* y ataques conexos.
	Ciberataque réplica	Se trata de ataques réplicas, realizados en el internet, de delitos que solían ejecutarse, de otro modo, en la realidad física. Los ciberataques replica pueden ser motivados por incentivos: a) económicos. Ej. los ciberfraudes; como *phishing, pharming, scam auction fraud*, el *cyberspyware*, el ciberblanqueo de capitales, la ciberextorsión, la ciberocupación. b) sociales. Ej. s*poofing*, *cyberstalking*, *cyberbulling*, *online harassment, online grooming*, y *sexting*. c) politicos. Ej. el ciberespionaje terrorista, y la ciberguerra (2013, p. 26).
	Ciberataque de contenido	Son aquellas conductas en las que el ilícito se centra en la transmisión de contenido a través de internet, la ilegalidad no se origina por el medio utilizado, sino por la distribución del contenido en internet. Ej. los delitos de distribución de pornografía infantil, comercialización de ciberpiratería intelectual, y difusión de contenidos ilícitos. El autor también considera que podría ubicarse en este bloque los cibercrímenes políticos de contenido como, por ejemplo; El *online hate speech*, y el ciberterrorismo en la modalidad de difusión de mensajes radicales con fines terroristas.

Fuente: Elaboración propia

En el presente trabajo se utilizará la terminología sistematizada por Miró, ya que es adecuada para visibilizar y plantear soluciones a la problemática de la cibercriminalidad pura en comparación con las clasificaciones de los demás autores. Es así como los autores citados no incluyen con claridad en sus clasificaciones valiosos criterios diferenciadores, como pueden ser las finalidades económicas, sociales, y políticas. Sin embargo, Miró considera que los cibercrímenes puros pueden perseguir finalidades económicas -*hacking*, *malware*, *virus*, ataques *DoS*- y políticas -ataques *DoS* a raíz de un *cyberwar*, o ataques *DoS* como resultado de *cyberhacktivism*-, ya sea de manera vinculada o independiente. Esta importante distinción que hace Miró en torno a la intencionalidad del cibercrimen en el ciberespacio -puro, réplica, contenido- otorga claridad sobre las razones -económicas, sociales, políticas- que pudieron influenciar a los cibercriminales en la comisión del ilícito. Por este motivo, como ya se dijo, se empleará su clasificación propuesta.

2. Cibercriminalidad pura

2.1 Concepto de cibercriminalidad pura

En el orden de lo antes visto, de acuerdo a Miró el cibercrimen puro es aquella modalidad o categoría delictiva situada dentro del fenómeno de la cibercriminalidad. La cual se distingue por ocurrir únicamente en el ciberespacio y no fuera de este (2011). Dicho de otra manera, la vertiente pura se caracteriza por lo siguiente:

- Es una actividad cibercriminal que, valiéndose del desarrollo y uso de las TIC, dirige el ciberataque hacia computadoras, programas informáticos -*software*-, redes, terminales y cualquier operatividad tecnológica basada en la comunicación digital de contenidos.
- No tiene una réplica en términos de referencia fuera del ciberespacio. Es decir, no es una réplica de delitos llevados a cabo en el mundo fáctico -ciberataque réplica-.
- la infracción normativa no está constituida por la comunicación con fines de propagación del contenido en internet -ciberataque de contenido-.

Sobre el concepto de ciberespacio, en tanto ámbito de comisión del ciberdelito es importante aclarar que, dado la peculiaridad de este entorno digital, algunos autores señalan que los ciberdelitos muchas veces se consuman en lugares que no tiene referente material en el mundo real, y por lo tanto no pueden llamarse propiamente un lugar, lo que conlleva a designarlos como ciber escenarios (De la cuesta y San juan, 2010; Mayer, 2018).

En esta línea, Schimitt (2013) señala que estos ciber escenarios del internet son espacios integrados por componentes tangibles e intangibles, donde abunda la conectividad entre redes computacionales y el espectro electromagnético, con el objetivo de transferir, modificar, y almacenar información.

De acuerdo con Zekos (2007), la virtualidad del internet o el también llamado ciber escenario se trataría de un espacio amorfo que no se tiene localización física y, por tanto, ocupa todo y, al mismo tiempo, nada. En sentido similar, Llorens (2017) señala que el ciberespacio se construye a partir de redes de *hardware*, *software* y datos interconectados a escala global mediante la interacción humana.

Entonces, se puede concluir que el ciberataque puro ocurre solamente dentro de una red globalmente interconectada de información digital e infraestructuras de las comunicaciones -concepto que normalmente se identifica con internet- y, más ampliamente, con las redes computacionales (Mayer, 2018).

2.2 Modalidades de la cibercriminalidad pura

La cibercriminalidad hace un uso intensivo de las TIC, por esa razón estas tienen un rol protagónico para entender la comisión de ciberdelitos en el ciberespacio, en consecuencia, las TIC conforman la infraestructura de internet, en tanto son los medios que viabilizan el funcionamiento de esta.

Como sostiene Miró, las TIC no son únicamente el conducto exclusivo por donde se realizan los ciberataques puros, sino que son el único medio posible, en la medida que son tanto medio como objetivo, y no es posible producir dichos ilícitos fuera del ciberespacio (2013). En efecto, a continuación, se caracterizarán tres modalidades de cibercrímenes que encajan adecuadamente bajo la denominación de cibercrimen o ciberataque puro.

2.2.1 Intrusión informática (*hacking*)

El *hacking* es conocido, también, como el acceso ilícito a sistemas informáticos. Este se produce cuando, mediante una entrada no autorizada por el administrador de un determinado sistema, un tercero accede a un sistema informático ajeno. Es así que, para que un cibercrimen sea considerado *hacking* "es necesaria la intervención de un tercero, mientras que, por el contrario, cuando el propio sistema envía información al *hacker* estaremos frente a otro tipo de cibercrimen" (2013, p. 55).

De otro lado, el *hacker* tiene que acceder de manera no autorizada sin el consentimiento del administrador del sistema, para tomar control de los privilegios administrativos, ya sea de manera parcial o total. El *hacking*, entonces, es una forma de "intrusismo informático" en la medida que la intromisión no autorizada a un sistema determinado menoscaba la esfera de privacidad y seguridad de los sujetos afectados.

2.2.2 Propagación de virus (*malware)*

De acuerdo con Dubrawsky, el concepto de *malware* es el siguiente:

> […] un virus informático se define como un programa informático auto replicante que

> interfiere con el *hardware*, *software* o sistema operativo de una computadora. El propósito principal de un virus es crear una copia de sí mismo. Los virus contienen suficiente información para replicarse y realizar otros daños, como eliminar, corromper o encriptar archivos importantes del sistema (2009, p.133).

Otra característica de este tipo de cibercrimen es que este virus debe, primero, ejecutarse y, posteriormente, la computadora tiene que cumplir las instrucciones que el virus brinda.

"Estas instrucciones -conocidas como el *payload* o carga útil del virus- pueden generar diversos efectos nocivos: interrumpir archivos de datos o cambiarlo, mostrar un mensaje o provocar un mal funcionamiento del sistema operativo" (p. 135).

Conviene precisar que las infecciones de *malware* hacen referencia a la capacidad de auto replica de *software* dañino que inserta líneas de código en los objetivos que daña (Mcafee, 2020).

La lista de la siguiente tabla 2 no pretende ser exhaustiva en su estudio por abarcar toda taxonomía de formas de propagación de virus informáticos, solo enumera los cinco subtipos más utilizados en la actualidad. Asimismo, cabe señalar que dentro del subgrupo de infecciones de *malware* también existen diversos subtipos que persiguen finalidades afines.

Tabla 2
Tipología de infecciones de malware

Fuente	Tipo de *malware*	Definición
Bederna y Szadeczky, 2019, p. 9-15.	*Worms*	Este virus ingresa a las computadoras a través de vulnerabilidades en el sistema y aprovechan las funciones de transporte de archivos o de información del sistema para desplazarse sin ayuda externa.
	Ramsomware	Es un *software* malicioso que bloquea acceso a datos o los filtra exigiendo a la víctima que para la liberación de estos se desembolse un rescate económico. Si la victima acepta las condiciones de la extorsión los ciberdelincuentes proceden con la desencriptación del cifrado.
	Spyware	También llamado programa espía, este *software* se construye con el objetivo de recopilar información privada sin el consentimiento o autorización del dueño.
	Rootkits	

		También llamado *software* encubridor, en la medida que permite esconderse en el sistema operativo con privilegios de acceso como si fueran administradores, al igual que lo haría el propietario del sistema.

Fuente: Elaboración propia

2.2.3 Ataques de denegación de servicios *(DoS y DDoS)*

Los ataques *DoS* también llamados ataques de denegación de servicio -*denial of service*- se caracterizan por inundar con solicitudes o paquetes -TCP y UDP- a un servidor en particular, sobresaturando su capacidad hasta que no pueda procesar el tráfico, y quede fuera de servicio. En consecuencia, esto resulta en la denegación de servicio para solicitudes adicionales (Overill, 1999).

Un ataque conexo al ataque de denegación de servicios -*DoS*- es el llamado ataque distribuido de denegación de servicios -*DDoS*- que se refiere al ataque común de denegación de servicios -*DoS*- pero de manera distribuida, es decir desde distintos puntos de conexión contra un objetivo de manera simultánea (Chandler, 2003).

Como se ha dicho el ataque distribuido de denegación de servicios -*DDoS*- se caracteriza por usar varios dispositivos distribuidos para aunarse a un ataque de denegación de servicios -*DoS*- prexistente. De acuerdo con las firmas de ciberseguridad y alta tecnología; CloudFlare, AT&T, y Cisco los ataques de denegación de servicios -*DoS*- pueden desplegarse de varias formas, algunos de estos ataques conexos incluyen los siguientes:

Tabla 3
Tipología de ataques de denegación de servicios

Fuente	Tipo de ataque	Concepto
	Ping of Death	El atacante tiene como objetivo interrumpir una máquina objetivo enviando un paquete más grande que el tamaño máximo permitido, haciendo que la máquina objetivo se congele o se bloquee.
	UDP Floods	Consiste en el envio de de paquetes de tipo -*UDP*- persiguiendo desgastar y por ende inutilizar la capacidad de procesamiento y respuesta del servidor atacado.
	Ping Flood	El atacante intenta agota los recursos disponibles de un dispositivo objetivo con paquetes de solicitudes, -*eco ICMP*- consiguiendo que el objetivo sea inaccesible para el tráfico normal.

Cloudflare, 2020; Cybersecurity AT&T 2020; Cisco 2020.		
	SYN Flood	El objetivo es consumir toda la energía disponible del servidor con la intención de quebrarlo o dejarlo inoperativo en términos de tráfico.
	Slowloris	Es un ataque de aplicación de capa que opera utilizando solicitudes *HTTP* parciales. El ataque funciona abriendo conexiones a un servidor *web* objetivo y luego manteniendo las conexiones abiertas el mayor tiempo posible.
	HTTP Flood	Esta diseñado para inundar el servidor objetivo con solicitudes *HTTP.*
	Brute-force Attacks	El atacante utiliza diversas técnicas y metodos para revelar datos confidenciales como claves secretas, APIs, etc.
	Zero-Day Attacks	Se origina cuando una vulnerabilidad de *software* es desconocida para todas las partes interesadas en repararla, incluidos los usuarios, los investigadores de seguridad y el equipo o desarrollador responsable del mantenimiento del proyecto.

Fuente: Elaboración propia

2.3 Crimen-Como-Servicio *(CaaS: Crime-as-a-Service)*

Es importante enfatizar que las modalidades del cibercrimen puro - como la intrusión informática (*Hacking*), la propagación de virus (*Malware*) y los ataques de denegación de servicios (*DoS*) - no, son necesariamente, supuestos de actividad criminal aislados en el tiempo y sin conexión entre delitos de similar naturaleza. Por el contrario mucha de la vasta actividad cibercriminal de vertiente pura se origina en ecosistemas criminales especializados que respaldan toda la cadena de valor del cibercrimen, además de impulsar la economía digital subterránea (Wainwright y Cilluffo, 2017).

La cibercriminalidad pura es una industria altamente rentable y con potencial de crecimiento exponencial, porque presenta características que han consolidado dicho crecimiento. Dentro de estas características se encuentran herramientas tecnológicas que facilitan a los ciberdelincuentes enmascarar su identidad, ubicación geográfica, datos personales, así como encriptar sus comunicaciones y ofuscar sus transacciones financieras (Ciancaglini, Balduzzi, McArdle y Rösler, 2015).

Al igual que el modelo de *software* como servicio -*SaaS*-, el -*CaaS*- permite que los productores logren economías de escala, lo que incidentalmente contribuye a la reducción de las barreras de entrada, en beneficio de nuevos participantes (Huang, Siegel y Madnick, 2017). Atendiendo a estas consideraciones, este fenómeno económico ha llevado al -*CaaS*- a expandir el alcance e intensidad del cibercrimen dentro de la sociedad moderna (Wilson, Schulman, Bankston y Herr, 2016).

Esta información es relevante de cara a valorar aquellas medidas político-criminales empleadas por el estado para hacerle frente y prevenir la actividad cibercriminal pura. Ello en la medida que a partir de este tipo de delincuencia se engendra una industria cibercriminal altamente integrada, dinámica y en continua evolución. Capaz de producir una amplia gama especializada de servicios y productos de índole comercial y complementarios (Wainwright y Cilluffo, 2017).

2.4 Concepto de ciberseguridad, estrategia de ciberseguridad, y ciber-potencia

Antes de ahondar en las diversas políticas de prevención contra el cibercrimen adoptadas en la actualidad, es adecuado definir los términos ciberseguridad, estrategia de ciberseguridad, y ciber-potencia. El termino ciberseguridad se refiere al conjunto de tecnologías, conceptos, políticas, procesos y prácticas utilizadas para proteger activos, por ejemplo; computadoras, infraestructura, aplicaciones, servicios, redes, sistemas de telecomunicaciones e información, y el ciber-entorno contra ataques, daños a la nación y acceso no autorizado (ITU 2008). En pocas palabras, la ciberseguridad es la "capacidad de protegerse a sí mismo y a sus instituciones contra ciber-amenazas" (Choucri, 2012, p. 13).

El término estrategia de ciberseguridad hace alusión a los planes y acciones ejecutados para alcanzar cierto nivel de ventaja competitiva nacional y desempeño superior en el frente de la ciberseguridad (Kshetri & Kshetri, 2016). Es así que la puesta en marcha de una ciberestrategia implica desarrollo tecnológico, y capacitación de la fuerza laboral específica para que trabajen dentro de la estrategia de ciberseguridad definida (Kshetri & Kshetri, 2016).

Por último, el termino ciber-potencia, según la interpretación de Kuehl (2009), sugiere “la capacidad de usar el ciberespacio de manera hegemónica para crear ventajas e

influir en eventos en diversos entornos operativos y en todos los instrumentos de poder "(p. 38). De acuerdo con Nye (2011), la idea es que una ciber-potencia es aquel Estado u organización política con la capacidad tecnológica suficiente para permitirse producir resultados deseados en el ciberespacio o en otros dominios.

3. Política criminal

3.1 Concepto de Política criminal

Entre las definiciones de política criminal. Roxin (2016) la define como los razonamientos valorativos de naturaleza jurídica fijado en las constituciones y en el derecho penal, que determinan los supuestos punibles y las sanciones correspondientes.

Con respecto a las definiciones extrapenales sobre política criminal, Jiménez de Asúa (1989) propone que esta es el resultado de la investigación de naturaleza científica basado en los componentes delictivos y punibles que emplea el derecho penal, así como los medios extra penales de carácter privativo.

Para Laura Zúñiga (2013) esta es una actuación política con respaldo estatal que aúna diversas estrategias de dimensiones complementarias con la misión de prevenir el crimen.

La definición empleada en la sentencia C-646 del 2001 de la corte constitucional colombiana, que luego fue acogida por la comisión asesora del observatorio de política criminal de aquel país, define a la política criminal como:

> […] el conjunto de respuestas que un Estado estima necesario adoptar para hacerles frente a conductas consideradas reprochables o causantes de perjuicio social con el fin de garantizar la protección de los intereses esenciales del Estado y de los derechos de los residentes en el territorio bajo su jurisdicción. Dicho conjunto de respuestas puede ser de la más variada índole. (Abadía, Romero, Lizarazo & Burgos, 2015, p. 4)

En una línea similar, Havican la define como el conjunto de intervenciones jurídicas y extrajurídicas, públicas y privadas, que tienen como fin prevenir o reducir la delincuencia o paliar los costes sociales del mismo (1999). Por otro lado, otros autores, desde un enfoque crítico, definen la política criminal como violencia estatal organizada -definición de Alberto Binder- (Abadía, Romero, Lizarazo, y Burgos, 2015, p. 4).

En este trabajo se empleará la definición de política criminal que refiere a la acción estatal que, dentro del marco de un Estado Constitucional de Derecho, se encamina a

resolver o enfrentar el problema de la criminalidad a través de la prevención del delito.

Se utilizará este concepto debido a que la prevención del delito es una política eficaz en la medida que se aproxima a las causas del conflicto que el delito exterioriza, de ahí se sigue que, a través de la prevención primaria, secundaria, y terciaria se ataca las raíces del conflicto que origina la delincuencia, en vez de incidir de manera tardía en los síntomas o manifestaciones exteriores del delito.

Una política criminal que enfatiza la prevención del delito busca exigir al Estado prestaciones positivas que neutralicen situaciones carenciales, conflictos, desequilibrios, y necesidades básicas, y no mera disuasión a través del derecho penal. Es así que para la prevención del delito el crimen se entiende como un problema social y comunitario, y no un cuerpo extraño ajeno a la sociedad, por ende, requiere estrategias preventivas con enfoques de tipo comunitario, situacional y del desarrollo.

Por las razones expuestas, el concepto antes visto se condice con la definición propuesta por la corte constitucional colombiana, ello en tanto la corte establece que la política criminal es el resultado de una pluralidad de manifestaciones, acciones, coordinaciones, y compromisos por parte del estado para proteger sus intereses y avalar la protección de los derechos de sus connacionales.

Por lo tanto, el conjunto de respuestas del Estado según la definición de la corte conlleva estrategias prevencionistas del delito de la más variada índole, pudiendo ser estas de corte, social, económico, cultural, administrativo, tecnológico, situacional, comunitario, del desarrollo, entre otras, además de jurídicas.

3.2 Enfoques de prevención primaria, secundaria y terciaria

Dentro de la prevención del delito como un conjunto de respuestas del Estado dentro de su política criminal se encuentran los enfoques de prevención primaria, secundaria, y terciaria, que se aproximan etiológicamente a las causas del conflicto que el delito exterioriza, a diferencia de la amenaza de la pena que al intervenir deja las causas intactas de la delincuencia, y no incide en las raíces del problema, sino solo en sus síntomas o manifestaciones tardías (García-Pablos de Molina, 2001).

Por un lado, se tiene que la amenaza de la pena enfatiza una forma de prevención puramente "negativa", o cuasi policial, sobre bases "disuasorias" que carece de operatividad, al no incidir en las causas del delito, además de actuar exclusivamente desde el derecho penal y no fuera de este.

Por otro lado, los enfoques preventivos del delito pueden operar tanto fuera como dentro del derecho penal, y la eficacia de estos radica en que actúan de manera inmediata, positiva y temprana en las causas mismas que originan el delito, de ahí que la prevención del delito no es lo mismo que dificultar la realización de ilícito, o desalentar al infractor con la amenaza de la pena, sino intervenir de manera temprana en el potencial conflicto criminal con la finalidad de prevenir el devenir del mismo.

Con respecto a los enfoques de prevención primaria, estos se orientan a las causas mismas, a la raíz, del conflicto criminal, persiguen neutralizarlo antes de que el problema se manifieste. Si bien actúa a mediano y largo plazo, requiere de prestaciones sociales y respuestas de diversa índole que posibiliten el bienestar social, además de identificar condiciones del entorno físico y social que influyen o precipiten la delincuencia.

Sobre el enfoque de prevención secundaria, este actúa más tarde en términos etiológicos, no cuando ni donde, el conflicto criminal se produce, sino cuando y donde se manifiesta o exterioriza. Actúa en el corto y mediano plazo y tiene como destinatarios a grupos de la sociedad proclives a protagonizar el problema criminal. Este enfoque se centra en la política penal y en la acción policial.

El enfoque de prevención terciaria, tiene un destinatario identificable: la población reclusa, penada; y un objetivo preciso: evitar la reincidencia. Actúa tarde sobre las causas que origina la criminalidad, y se centra en programas de carácter rehabilitador o resocializador que se realizan en centros penitenciarios.

3.3 Política criminal y las estrategias de prevención del delito

Los programas de prevención del delito pueden actuar tanto fuera como dentro del sistema penal. De esta forma, los mecanismos de prevención del delito se multiplican y actúan de manera holística, confluente o integrada. Para Tonry (2011) hay tres principales estrategias de prevención del delito: prevención situacional, del desarrollo y

comunitaria. Cuando estas estrategias operan fuera de los confines del sistema penal, se vuelven una forma alternativa y eficaz de reducir la delincuencia (Welsh, Farrington y Gowar, 2015).

3.3.1 Prevención situacional

La prevención situacional se refiere a las intervenciones diseñadas para prevenir la ocurrencia de delitos mediante la reducción de oportunidades, aumento del riesgo y la dificultad de ofender (Cornish y Clarke, 2003; Welsh y Farrington, 2012).

Los programas de prevención situacional reducen las tasas de delitos que se cometen de manera impulsiva y sin desplazamiento a otros lugares. Esto implica la implementación de medidas de seguridad en aquellos lugares donde el delito es una actividad frecuente.

Estas medidas pueden manifestarse en la forma de "instalaciones de vidrios a prueba de balas, circuitos cerrados de televisión, mejor iluminación, políticas de cambio en autobuses y tranvías, y un conjunto de otras iniciativas que hacen que los delitos sean más difíciles de cometer" (Tonry, 2011, p. 7).

Para Summers (2009) el enfoque de la prevención situacional de delito establece que el ilícito no se manifiesta de forma aleatoria en el espacio o en el tiempo, sino que "existen lugares y períodos específicos en los que el delito es más prevalente, por ejemplo, en zonas de ocio nocturno los fines de semana" (p. 396).

En esta línea el autor enfatiza que la importancia del contexto y los factores ambientales tienen un rol importante para determinar los motivos que incentivan al delincuente a delinquir. Esta línea de razonamiento considera al delincuente como un ser relativamente racional, que basaría su actuar en un análisis de los daños y beneficios que conllevaría delinquir.

De ahí se sigue que la estrategia de prevención situacional modifica los entornos medio ambientales a través del incremento de daños potenciales, y la mitigación de los beneficios del delinquir, de esta manera busca aminorar las oportunidades o el atractivo de la actividad delincuencial.

3.3.2 Prevención del desarrollo

Se refiere a las intervenciones diseñadas para prevenir el desarrollo del potencial criminal en individuos, y está dirigido especialmente a personas con factores de riesgo y protección según estudios de desarrollo humano (Tremblay y Craig, 1995; Farrington y Welsh, 2007).

De acuerdo con Tonry (2011) los programas preventivos del desarrollo reducen la probabilidad de delinquir de niños en riesgo. Estos programas identifican los factores de riesgo y protección en la vida de los niños con la finalidad de debilitar los primeros, mientras fortalecen los segundos.

Programas de este tipo incentivan intervenciones que mejoran las habilidades de crianza de padres con niños en riesgo, así como estrategias que producen mejoras de la salud física, mental, y del rendimiento escolar. De igual manera se incluyen intervenciones dirigidas a reducir cualquier forma de abuso infantil, con la finalidad de mitigar las probabilidades de delinquir años después.

De acuerdo a Aos, Miller y Drake 2006 la inversión pública en programas de prevención del desarrollo es mucho más rentable, entre tres a cuatro veces más que la inversión en sentencias de prisión. Desafortunadamente, la inversión en este tipo de programas resulta rentable en un marco de tiempo de diez a quince años después de haberse implementado.

Situación que según Tonry (2011) genera un desincentivo para la clase política debido a que “no es el período de referencia que la mayoría de políticos tiene en mente, al proponer legislación preventiva y luego votar por provisiones de fondos para financiarla” (p. 7).

3.3.3 Prevención comunitaria

Se refiere a intervenciones diseñadas para cambiar las condiciones e instituciones sociales, por ejemplo; familias, pares, normas sociales, clubes, y organizaciones que influyen en la delincuencia de las comunidades residenciales (Hope, 1995; Welsh y Farrington, 2012).

Para Farrington (1995) es posible reconocer la existencia de superposición en los límites

de la prevención comunitaria y del desarrollo, así como en los límites de la prevención comunitaria y situacional. De lo cual se infiere que las estrategias de prevención del delito no son una clasificación estanca.

Tonry (2011) señala que la prevención comunitaria se divide mayormente en dos formas, la primera es la creación de organizaciones comunitarias de autoayuda para la prevención del delito, estas organizaciones operan bajo alguna permutación del nombre “vigilancia vecinal".

La segunda forma se trata de la prevención del delito situacional a nivel comunitario y arquitectónico. Iniciativas a nivel comunitario incluyen medidas como el mejoramiento del alumbrado público, la alteración de los patrones de flujo de tráfico y el cierre de calles mediante rejas.

Iniciativas a nivel arquitectónico pueden incluir medidas como la construcción de "espacios defendibles" con líneas de visión claras, y oportunidades de vigilancia que permite a residentes ver la actividad que sucede en el barrio y en las inmediaciones.

3.4 Medidas de prevención cibercriminal

Según Dupont (2019), a pesar de las importantes inversiones realizadas por los gobiernos durante la última década para mejorar la ciberseguridad de los sistemas informáticos públicos y privados, todavía existe un conocimiento sistemático muy limitado sobre qué políticas y/o medidas de prevención en torno al cibercrimen se han adoptado en varias partes del mundo. Aunado a esto, se desconoce la efectividad de las medidas implementadas para controlar la exposición y reducción del cibercrimen entre individuos y organizaciones. A continuación, se plantearán cuatro propuestas de prevención del delito, empleadas en la actualidad como parte esencial de estrategias internacionales para combatir el cibercrimen y asegurar la ciberseguridad.

3.4.1 Auto-Regulación y Co-Regulación de asociaciones público-privadas

Tabla 4
Auto-Regulación y Co-Regulación de asociaciones público-privadas

Autores y año	**Tropina y Callanan (2015)**
Objetivo	Los autores recomiendan desarrollar y fortalecer mecanismos de auto-regulación, que se refieren a las iniciativas de coordinación iniciada por actores privados no jerárquicamente organizados y establecidos independientemente de la adopción de

	órdenes legales, por ende, bajo un enfoque de abajo-arriba -*bottom-up*-, y mecanismos de co-regulación que supone la participación directa de los actores públicos en el proceso regulatorio, por ende bajo un enfoque de arriba-abajo -*top-down*-. Los mecanismos de auto-regulación y co-regulación de asociaciones público-privadas, conllevan un componente necesario que permite complementar la ley penal, y no ser una alternativa a esta última, funcionando entonces como una capa adicional a la legislación aplicable, a la vez que fortalecen una dinámica participativa sólida entre los actores estatales y los privados, en beneficio de mejorar las capacidades de ciberseguridad de las asociaciones de ambos sectores en la lucha contra el cibercrimen. Ejemplos de auto-regulación de asociaciones público-privadas incluye desde colaboración ad hoc a solicitud de la policía en materia de ciberseguridad, hasta asociaciones y organizaciones industriales que implementan diferentes mecanismos de auto-regulación dentro de sus procesos, muchas formas de auto-regulación incluyen al estado como iniciador o participante. Ejemplos de co-regulación son aquellos que requiere la participación y cumplimiento estatal, puede tomar la forma de creación de diferentes organizaciones, asociaciones, y foros, durante la elaboración de acuerdos entre proveedores de servicios de internet y agencias de las fuerzas del orden, o plataformas de denuncia que llevan a cabo campañas de sensibilización.

Fuente: Tropina y Callanan (2015), p. 9-109. Elaboración propia

Los autores proponen con los modelos de co-regulacion y auto-regulacion medidas de prevención situacional que vinculan el esfuerzo conjunto del sector público y privado para obstaculizar la comisión del ciberdelito, aunque debe observarse que si el componente co-regulatorio *top-down* propuesto necesite criminalizar conductas o modificar penas, entonces la iniciativa se situaría simultáneamente dentro del enfoque secundario de prevención del delito.

El despliegue sinérgico de ambos mecanismos regulatorios ofrece un efecto disuasorio a través de instrumentos penales y no penales. Por consiguiente, esta propuesta mitiga las oportunidades de cometer cibercrímenes mediante mecanismos neutralizadores propios de las asociaciones público-privadas, estrategias de este tipo operan dentro de la prevención situacional del delito.

3.4.2 Privatización de la ciberseguridad

Tabla 5
Privatización de la ciberseguridad

Autores y año	**Sales (2018)**
Objetivo	La privatización de la ciberseguridad para Sales implica lo siguiente: Incentivar a *hackers* a vender errores/fallas (*bugs*) en el mercado blanco a proveedores que los parcharán, en lugar de venderlos a las agencias gubernamentales (mercado gris) y cibercriminales (mercado negro) que planean explotarlos. En la actualidad los *hackers* prefieren como primera opción vender los *bugs* en el mercado gris (*grey market*) donde el más grande comprador es el gobierno, a través

	de sus agencias (NSA, CIA) porque los pagos son lucrativos. La finalidad de estas compras gubernamentales obedecería a estrategias ofensivas como recopilación de información, operaciones encubiertas, rastreo de objetivos, etc. Como segunda opción los *hackers* comercializan *bugs* en el inescrupuloso mercado negro (*black market*) donde el colectivo cibercriminal es el segundo mejor comprador (compuesto mayormente por organizaciones internacionales, gobiernos extranjeros hostiles, grupos terroristas, entre otros). Como última opción ya sea por consideraciones éticas o investigativas los *hackers* venden *bugs* en el mercado blanco (*white market*) con la intención que los proveedores de *software* parchen aquellas fallas/errores y por lo tanto no las exploten. El problema estructural del mercado blanco es que esta poco desarrollado en la medida que se ofrece pagos modestos por *bugs*, o por lo venta de información relacionada a vulnerabilidades de *software*. El mercado blanco presenta imperfecciones típicas de mercados pocos desarrollados como altos costos transaccionales, y defectos estructurales. Es así como los *hackers* prefieren vender *bugs* a los otros mercados por estar más desarrollados y ofrecer mejores pagos. Como resultado se venden menos *bugs* a los proveedores de *software*, estos no se reparan o parchan oportunamente, y los usuarios permanecen expuestos a ciberataques.

Fuente: Sales (2018), p. 622-688. Elaboración propia

Sales afirma que, si los formuladores de políticas desarrollan los incentivos adecuados para que el mercado blanco pueda prosperar, las asimetrías, imperfecciones y defectos actuales propias del subdesarrollo serían reemplazados por un círculo virtuoso de buenas prácticas, y así de manera progresiva se mejoraría la seguridad del producto -*software*-, mientras se reduce el volumen de ventas de los mercados con los que compite.

Sales propone una solución de tipo co-regulatorio -*top-down*-, en la medida que requiere la intervención y observancia estatal como componente necesario para su implementación. Es así que Sales coincide con los autores Tropina y Callanan cuando sugieren que resultaría un error por parte del sector público descuidar la importancia de consolidar una sinergia con el sector privado, en la medida que el papel fundamental del gobierno es la de desempeñar liderazgo de la seguridad en el ciberespacio.

Esta propuesta es un tipo de estrategia situacional del delito, debido a que se aboca a mejorar las disparidades de precios existentes en mercados lucrativos como el gris -*grey market*- y el negro -*black market*- en comparación con el blanco -*white market*-, mediante financiación pública en la forma de protecciones de responsabilidad -*liability protections*-, beneficios fiscales y subsidios directos.

Sin embargo, en la medida que se requiera criminalizar alguna conducta relacionada a la venta de errores/fallas -*bugs*- en el mercado gris -*grey market*- y negro -*black market*- respectivamente, en vez de hacerlo en el mercado blanco -*white market*-, o la modificación de alguna pena en torno a las actividades conducidas en dichos mercados,

entonces se estaría aplicando de manera concurrente normativa jurídico penal propia del enfoque secundario de prevención del delito.

Finalmente, esta iniciativa buscaría compatibilizar distintos objetivos prevencionistas en el mercado blanco como, por ejemplo, la subversión de las reglas establecidas de compra y venta en el mercado ilegal negro en la forma de disminuir las ganancias de este último, o en el gris en la forma de eliminar excusas a la hora de realizar ventas en este mercado donde dichas transacciones conllevan una garantía implícita de inmunidad de responsabilidad civil y penal.

3.4.3 Monitoreo preventivo del cibercrimen

Tabla 6
Monitoreo preventivo del cibercrimen

Autores y año	**Dupont (2019)**
Objetivo	El monitoreo preventivo consiste en utilizar el potencial de las herramientas de monitoreo para cerrar la brecha en torno al desconocimiento de políticas, modelos, propuestas, o programas para combatir el cibercrimen alrededor del mundo. La utilización de las herramientas de monitoreo preventivo permitiría a la ciudadanía y a los legisladores contar con conocimiento idóneo para determinar cuáles serían las iniciativas de intervención gubernamental o del sector privado más eficientes para controlar, combatir, y/o mitigar los daños causados en el ciberespacio. El monitoreo preventivo buscaría conseguir los siguientes objetivos: • Provisionar métricas estrictas que detallen los hitos alcanzados de aquellas políticas destinadas a combatir el cibercrimen. • Realizar un análisis granular de carácter científico para establecer qué políticas y programas ofrecen mejoras cuantificables para la seguridad del ecosistema digital. • Revertir el escenario en el cual algunas plataformas importantes, y organizaciones internacionales han desarrollado iniciativas ambiciosas para proteger a sus connacionales, mientras aún existe el desconocimiento generalizado sobre qué políticas ya están siendo implementadas por qué países, a qué costo y con qué resultados.

Fuente: Dupont (2019), p. 500-515. Elaboración propia

El planteamiento del monitoreo preventivo es una estrategia de prevención que puede tomar la forma de vertiente situacional, comunitaria, y del desarrollo. Debido que a partir del acopio del conocimiento idóneo para determinar las iniciativas de intervención gubernamental o del sector privado más eficientes, se estaría de manera conjunta desplegando varias políticas probadas que controlen, combatan, y/o mitigen los daños causados por la cibercriminalidad.

El monitoreo preventivo se subsume al grupo de técnicas de prevención del delito debido a la sumatoria de esfuerzos de corte científico, legal, técnico, y social, que al ser empleados de manera conjunta combatirían la naturaleza multidisciplinar del fenómeno de la cibercriminalidad. Por lo tanto, el monitoreo preventivo posibilitaría la movilización

de diversas competencias.

3.4.4 El daño extracontractual de la habilitación negligente del ciberdelito

Tabla 7
El daño extracontractual de la habilitación negligente del ciberdelito

Autores y año	**Rustad y Koenig (2005)**
Objetivo	La propuesta de Rustad y Koenig busca responsabilizar a los proveedores de *software* por productos y servicios tecnológicos defectuosos que allanan el camino para que delincuentes exploten conocidas vulnerabilidades. Los autores proponen un deber de cuidado modificado que asegure la producción de *software* seguro y adecuado en el respectivo entorno de uso. Los autores proponen que la legislativa extracontractual estadounidense proponga la implementación de un "deber de cuidado" requerido para la producción de *software* seguro que proporcione a los proveedores y otras partes interesadas incentivos necesarios para implementar, instalar y actualizar productos y servicios de *software* que sean seguros y confiables. Si bien los consumidores deben tener ciertos cuidados para evitar el spam, las infecciones de *malware*, y otros cibercrímenes, los autores señalan que el rol de las cortes es de articular tal deber de cuidado para que el *software* vendido por los fabricantes no avance la agenda cibercriminal de manera indirecta. Los autores establecen que la industria del *software* debe brindar un "deber de cuidado razonable" a la hora de proteger a los usuarios de cibercrímenes altamente previsibles, como por ejemplo, la eliminación de prácticas de diseños negligentes, y la instalación de servicios de seguridad de Internet inadecuados y cortafuegos mal configurados. Dicho de otra manera, la responsabilidad extracontractual debería recaer en cabeza de los proveedores de la industria, por no haber implementado los medios disponibles para prevenir ciberdelitos previsibles. Los autores señalan que al igual que los casos de responsabilidad civil de predios, las cortes deberían imponer responsabilidad basada en negligencia por parte de los proveedores, al no haber implementado medios disponibles que aseguren la protección de sus clientes, y así evitar la comisión de ciberdelitos mediante el uso ilegal del *software*.

Fuente: Rustad y Koenig (2005), p. 1553-1612. Elaboración propia

La promulgación de una ley que busca establecer una categoría nueva de daños extracontractuales encajaría como una estrategia de prevención situacional, porque se vería plasmada en la normativa civil sobre reparaciones del daño o responsabilidad extracontractual.

Esta categoría de daño extracontractual estaría dentro de las técnicas de prevención situacional, en la medida que los daños causados por el código inseguro se originarían en supuestos de negligencia extracontractual, el cual habría posibilitado la explotación de vulnerabilidades por los ciberdelincuentes.

Es así que al implementar normativa civil sobre reparación de daños extracontractuales

se estaría "aumentando el esfuerzo" de cibercriminales para que no tengan la ventaja de explotar vulnerabilidades de *software* que podrían haber sido descubiertas a tiempo, como por ejemplo al haberse endurecido las medidas de seguridad por parte del fabricante del producto defectuoso, antes que este salga a la venta.

De ahí se infiere que la comisión del ilícito parecería más difícil o como menciona Summers (2009) la apariencia que lo es comunicaría al delincuente la considerable dificultad de delinquir, conviertiendose esta lectura del potencial delincuente en el móvil disuasor fundamental de toda campaña exitosa de prevención.

4. Conclusiones

- El cibercrimen es cualquier actividad delictiva que involucre una computadora como instrumento, objetivo o medio para perpetuar más delitos. Bajo una interpretación amplia del término cibercrimen este incluiría cualquier comportamiento delictivo realizado en el ciberespacio que no podría haberse dado fuera de él. Pero bajo una interpretación restrictiva, el criterio clasificador dependería de aquel establecido por el autor, el cual podría responder a diversa índole de aspectos y consideraciones.

- El concepto de cibercriminalidad pura se refiere a toda aquella actividad cibercriminal que solo puede ocurrir únicamente en el ciberespacio y no fuera de este, como puede ser la cibercriminalidad de vertiente replica y, o de contenido.

- Las modalidades de la cibercriminalidad pura incluyen: la intrusión informática (*hacking*), la propagación de virus (*malware*), y los ataques de denegación de servicios (*DoS*). La actividad cibercriminal pura con frecuencia se origina en ecosistemas cibercriminales especializados que respaldan toda la cadena de valor del cibercrimen, además de impulsar la economía digital subterránea, un ejemplo de esto es la modalidad llamada "crimen como servicio".

- La política criminal empleada en este trabajo es aquella que bajo la cual toda acción estatal se encuentra enmarcada en el modelo de Estado Constitucional de Derecho, y atiende el problema de la criminalidad a través de la prevención

del delito. Se dijo que este concepto de política criminal considera la prevención de delito como la vía idónea para hacerle frente a la ciberdelincuencia.

- Se dijo que los programas de prevención se dividen en primarios, secundarios, y terciarios, los primeros abordan las causas estructurales del conflicto criminal con la finalidad de contrarrestarlos, los segundos se dirigen donde el delito se manifiesta o exterioriza y opera en sectores concretos de la sociedad, los últimos se enfocan en la población encarcelada y buscan evitar la reincidencia.

- Sobre las estrategias de prevención del delito estas pueden ser de tipo situacional; que son intervenciones diseñadas para prevenir la ocurrencia de delitos mediante la reducción de oportunidades, aumento del riesgo y la dificultad de ofender, o del desarrollo; que se refiere a las intervenciones diseñadas para prevenir el desarrollo del potencial criminal en individuos, y está dirigido especialmente a personas con factores de riesgo, o incluso pueden ser comunitarias; que se refiere a aquellas intervenciones diseñadas para cambiar las condiciones e instituciones sociales, y arquitectónicas que influyen en la delincuencia dentro de comunidades.

- Las cuatro propuestas presentadas en la actualidad para combatir el cibercrimen no encajan necesariamente dentro de la tipología de programas de prevención primaria, que tienden a ser mayormente programas de prestaciones sociales y respuestas de diversa índole que posibiliten el bienestar social, además de identificar factores sociales que influyen o precipiten la delincuencia. De ahí que al no orientarse a las causas mismas del conflicto criminal (el cuándo y dónde), las propuestas no pretenden resolver de manera directa situaciones carenciales criminógenas o problemas de índole estructural, entre otros factores de corte pluricausal, que son temas de competencia del Estado y de su política criminal vigente.

- Las propuestas para combatir el cibercrimen operarían más tarde en términos etiológicos, además de operar de manera selectiva, en aquellos espacios donde la cibercriminalidad se exterioriza. De acuerdo a la política criminal de cada país, estas iniciativas para combatir la cibercriminalidad podrían situarse dentro de los ámbitos de la aplicación de la ley penal, la prevención del delito (comunitaria, desarrollo, situacional), y/o la regulación.

- Con respecto a las estrategias de los programas propuestos, estas son mayormente intervenciones preventivas del tipo situacional y comunitario dado que persiguen neutralizar la ocurrencia del ciberdelito. De esta manera los programas basan sus ideas centrales no en aquellas razones que convierten a una persona en delincuente, sino en las circunstancias del entorno social en las que delinquen y como poder decrecer los chances con el propósito de rehabitarlos.

- Como se ha visto las propuestas para combatir la cibercriminalidad no distingue entre las vertientes del cibercrimen; puro, replica, y contenido, esto es así porque las soluciones resultan aplicables a cualquiera de ellas sin distinción, en tanto se realice una adecuada ejecución e implementación de dichos modelos, se deduce que las tasas de actividad cibercriminal disminuirían en su conjunto.

- Estas iniciativas de prevención del delito buscan incidir en la política criminal de un país para poder hacer frente y/o prevenir la cibercriminalidad, de ahí se sigue que sin soluciones programáticas de este tipo o similares, la política criminal de un país no podría combatir la ciberdelincuencia de manera efectiva, en tanto carecería de las herramientas científicas, legales, técnicas, sociales, y demás para combatir de manera holística, integrada, o conjunta la naturaleza multidisciplinar del fenómeno cibercriminal.

CAPÍTULO 2
Aproximación criminológica a la cibercriminalidad pura

1. Investigación criminológica y cibercriminalidad pura

La investigación criminológica ha expandido su enfoque en las últimas dos décadas para mejorar el conocimiento del impacto tecnológico en las prácticas delincuenciales, los factores que afectan el riesgo de victimización y la aplicabilidad de teorías tradicionales del delito a los nuevos delitos virtuales (Miller, 2020).

Aunque el volumen de estudios realizados a la fecha ha mejorado en gran medida el conocimiento sobre el crimen facilitado por la tecnología o cibercrimen, todavía es crucial analizar de manera selectiva la literatura especializada debido al rango de perspectivas metodológicas, y teóricas que se han empleado para determinar los hallazgos (Holt y Bossler, 2014).

En esta línea, algunas investigaciones cualitativas han desarrollado conjuntos de datos para examinar las poblaciones infractoras en espacios virtuales, otras investigaciones cuantitativas han empleado la logística binaria y modelos de regresión múltiple generados a partir de muestreos de estudiantes universitarios (Higgins, Fell y Wilson, 2006). Mientras que otros han empleado técnicas de modelado de ecuaciones estructurales a un pequeño número de análisis descriptivos de grandes muestras representativas juveniles (Higgins et al., 2006).

Incluso existen estudios que han aplicado varias teorías criminológicas tradicionales a múltiples formas de cibercrimen con distintas operacionalizaciones. En consecuencia, las diversas modalidades investigativas dificultan evaluar el impacto general del fenómeno de estudio en el campo (Holt y Bossler, 2014).

De acuerdo con la Oficina de Naciones Unidas contra la Droga y el Delito -UNODC-, la conducta delictiva puede emanar de diferentes tipos de influencias causales, como se explica en los enfoques ético, clásico, positivista y estructural. Es así que, bajo el enfoque ético, la conducta criminal otorga satisfacción en vez de vergüenza. Para el estructural las condiciones políticas, económicas, y sociales crean entornos conducentes para la comisión de conductas reprochables. Mientras que para el enfoque clásico los factores facilitadores del crimen estarían asociados con decisiones de libre determinación que maximizan el placer y evitan el castigo, y para el positivista: las

influencias sociales y económicas incentivarían a las personas por el sendero criminal (UNODC, 2020).

Como se puede inferir a partir de los diversos tipos de influencias causales el crimen tiene una dimensión multicausal. En esta línea Herbert señala lo siguiente:

> […] si bien la criminología ha fomentado muchas teorías sin una falta significativa de consenso. La mayoría de criminólogos adopta una explicación "multifactorial", en la medida que no existe una explicación causal única para la criminalidad, sino un "paquete" de condiciones interrelacionadas de aplicabilidad variable (1982, p. 341).

En el mismo sentido, Gorecki precisa que:

> […] el crimen no puede explicarse en términos de una o algunas condiciones. Debido a la heterogeneidad de la conducta delictiva, el número de sus condiciones suficientes y sus componentes esenciales es casi ilimitado, incluso en un nivel cercano a la distancia causal (1974, p. 464).

De esta forma, el cibercrimen, al igual que toda manifestación criminal es multicausal. En este sentido, la teoría criminológica permite explicar la relación causal entre aquellos factores identificados en la evidencia empírica de los estudios y su correlación con el cibercrimen. Como sostiene Serrano Maíllo (2016) la mayoría de las teorías criminológicas son explicaciones de base ancha, y en algunos casos puntuales, postulan de manera deductiva hipótesis precisas y coherentes entre sí que pueden someterse a la refutación y superarla. Es así como las teorías criminológicas enfatizan factores de distinto nivel como pueden ser aquellos de índole macrosocial, micro social, y del historial personal.

Las macro teorías del comportamiento delictivo explican el panorama general del delito en todo el mundo o en una sociedad. Intentan responder por qué existen variaciones en las tasas de delincuencia de grupos. Algunos autores para referirse a las macro teorías han utilizado los términos “epidemiología o teorías de la estructura social” (Akers, 2013, p.3).

Las micro teorías del comportamiento delictivo se centran en un pequeño grupo de delincuentes o en un delito individual. Intentan responder por qué algunas personas tienen más probabilidades que otras de cometer un delito. Algunos autores para referirse a las micro teorías han utilizado los términos "conducta individual o teorías procesuales” (p. 4).

A continuación, se presentará un grupo de teorías criminológicas que explican el fenómeno de la cibercriminalidad. Se advierte, que no todas ahondan en la modalidad pura exclusivamente. Esto se debe a que la definición de cibercriminalidad pura es una clasificación arbitraria de un subtipo que se subsume dentro del cibercrimen. Es así, que desde un enfoque criminológico de alcance holístico o integrado, se considera que las conclusiones arribadas en dichos estudios resultan aplicables y en cierta medida adecuadas a los ciberdelitos puros.

2. Teorías del control

Dentro de las teorías del control, aquellas que hacen referencia a la capacidad del individuo de auto controlarse, dentro de entornos que podrían "aflojar" dicha capacidad, propiciando así la participación en actividades delincuenciales, se sitúa la teoría del autocontrol propuesta por Gottfredson y Hirschi (1984).

2.1 Teoría del autocontrol

Gottfredson y Hirschi propusieron en 1984 la teoría del autocontrol, la cual señala que una baja capacidad de auto controlarse al interactuar con la oportunidad criminal es la principal causa del crimen. El énfasis de esta teoría recae en la primera socialización de los niños durante la infancia y dentro de la familia, que en opinión de los autores produciría una predisposición criminal duradera a lo largo de sus vidas, llamado bajo autocontrol (Grasmick, Tittle, Bursik, y Arneklev, 1993).

El llamado bajo autocontrol es un rasgo unidimensional que consiste en impulsividad, preferencia por tareas simples en lugar de complejas, búsqueda de riesgos, preferencia por el uso del cuerpo o del físico y no por incentivos de tipo intelectual, "una orientación egocéntrica y un temperamento volátil" (Grasmick et al., 1993, p. 6).

La teoría del autocontrol considera que la motivación para cometer un delito no es una variable. Más bien, todos los actores son racionales y están motivados para perseguir su propio interés, incluida la comisión del delito. Lo que varía entre los individuos es su nivel de autocontrol y su acceso a oportunidades para delinquir, pero ni el bajo autocontrol ni la existencia de oportunidades delictivas por sí mismas son los principales determinantes de la delincuencia. En cambio, es la combinación de ambos componentes; llámese bajo autocontrol y efecto de interacción con la existencia de

oportunidades delictivas, lo que daría como resultado el comportamiento delictivo (Grasmick et al., 1993).

La teoría de Gottfredson y Hirschi (1984) ha sido utilizada por distintos autores para investigar en qué medida se podría configurar una relación entre la participación en actividades de piratería, ya sea que implique la descarga ilegal de música, películas, o software. Asimismo, se ha utilizado para validar si existe alguna correlación entre un bajo nivel de autocontrol y la participación en actividades de *hacking*. A continuación, se visualizarán algunos de los estudios que han aplicado la teoría del autocontrol para entender los ciberdelitos de piratería en línea.

Tabla 8
Estudios piratería digital y hacking

Estudio	**Higgins, Fell, y Wilson (2006)**	**Holt, Cale, Brewer, Goldsmith (2021)**
Objetivo	Medir el vínculo entre la piratería digital (música, películas, y *software*) y una capacidad de bajo autocontrol y de aprendizaje social.	Se busco identificar de qué manera la capacidad de autocontrol y la oportunidad influyen en el riesgo de participar de actividades de *hacking* entre demográficos adolescentes y juveniles. Se crearon una serie de variables independientes para evaluar las relaciones entre oportunidad, bajo autocontrol y cibercriminalidad.
Metodología	Cuestionario de autoinforme a población universitaria, las respuestas fueron anónimas y confidenciales. El análisis se basó en modelos de ecuaciones estructurales.	Cuestionario de autoinforme administrado en 18 escuelas como parte de una encuesta longitudinal de adolescentes australianos. La muestra representó el 37,5% de todas las escuelas públicas ubicadas dentro de la región. El análisis se basó en modelos de regresión logística binaria.
Conclusiones	El vínculo entre el bajo autocontrol y la teoría del aprendizaje social sugiere que aquellos individuos con bajo autocontrol aprendan a piratear digitalmente. Además, es probable que aquellos que han aprendido a piratear digitalmente pirateen *software*. Aunque la piratería digital no es un acto físico, puede proporcionar al individuo con bajo autocontrol una sensación de aventura, emoción o incluso riesgo.	Los hallazgos refuerzan la noción que el bajo autocontrol se asoció significativamente con dos formas muy básicas de *hacking* como: (1) acceder al dispositivo de otra persona sin su permiso para eliminar o modificar información o agregar archivos (2) acceder a la cuenta en línea de otra persona sin su permiso para eliminar o modificar información, o agregar archivos. Dado que el análisis se centró en modalidades simples de *hacking*, es muy posible que tener un bajo autocontrol no sea aplicable a las modalidades más sofisticadas. Por lo tanto, no se midieron habilidades complejas, como la creación de *malware* o el robo de información financiera.

Fuente : Higgins et al., 2006, pp. 19-22 ; Holt et al., 2021, pp.681-684. Elaboración propia

2.2 Teoría de los vínculos sociales

La teoría del control o de los vínculos sociales fue propuesta por Travis Hirschi (1969). Esta no buscaba explicar los motivos subyacentes que originaban la delincuencia, sino aquellos que impedían la violación de la ley. Dicho de otra manera, la teoría buscaba mostrar que factores influían para que las personas no delincan. En esta medida, Hirchi resaltó que el factor principal para que los seres humanos no delincan se encuentra en la internalización de las normas, esto es, en el control social (p. 18).

Como indica Sims (2002, p.102), Hirchi reconoce cuatro elementos necesarios para engendrar el control social :

a. Apego: las personas que están más unidas a los demás como familiares y amigos, por ejemplo, serían más propensos a seguir las normas de la sociedad. El apego se puede mostrar cuando alguien es sensible a la opinión de los demás sobre su comportamiento.
b. Compromiso: las personas se comprometen cuando les importa lo que podrían perder si cometieran actos delictivos. Cosas como posesiones, reputación y oportunidades podrían perderse si deciden delinquir. En consecuencia, aquellos con un mayor compromiso hacia las cosas que han logrado o desean lograr tendrían menos probabilidades de infringir la ley.
c. Participación: las personas que participan en actividades no delincuenciales, estarían mayormente ocupadas y tendrían menos oportunidades de cometer conductas delictivas.
d. Creencias: las personas con mayor creencia en las leyes, las acatarían. Mientras que, por otro lado, aquellos que no tienen una actitud de respeto hacia ellas podrían no sentir ninguna obligación moral de adecuarse a estas, independientemente que les origine una ventaja personal o no.

A continuación, se verá como un estudio aplicó la mencionada teoría para explicar la cibercriminalidad:

Tabla 9
Estudio Hacking juvenil

Estudio	**Back, Soor, LaPrade (2018)**
Objetivo	La hipótesis de trabajo buscaba confirmar o negar si la teoría del autocontrol y la de los vínculos sociales eran predictores significativos para la comisión de cibercrímenes.

Metodología	La recopilación de datos se completó en 31 países agrupados por diversas regiones geográficas. Los participantes en la encuesta de autoinforme fueron 68,507 estudiantes de los grados 7, 8 y 9 entre las edades de 11 a 16 años, se empleó la metodología de análisis de regresión logística multivariable.
Conclusiones	Los resultados indicaron que el bajo autocontrol es un fuerte predictor de *hacking* juvenil en todo el mundo, y los lazos sociales también son un predictor, aunque no de manera consistente. Los adolescentes que tenían un fuerte apego a la supervisión parental mostraron menos probabilidades de participar en *hacking*. Lo que demostró que el apego a la supervisión parental reduce la probabilidad de *hacking* en un 22%. Los resultados apoyan parcialmente la noción que un fuerte vínculo académico por parte de los jóvenes atenuaría la probabilidad de *hacking* en un 21%. Finalmente, los resultados indicaron que el género es un predictor muy fuerte de *hacking* juvenil. Siendo así que los adolescentes varones tienen mayores probabilidades de participar en *hacking* que las mujeres adolescentes de la misma edad. Por lo tanto, los hallazgos brindan un fuerte apoyo a la teoría del autocontrol de Gottfredson y Hirschi (1990) y un apoyo parcial a la teoría del vínculo social de Hirschi (1969).

Fuente: Back et al., 2018, p. 44-49. Elaboración propia

2.3 Teoría de la deriva digital

Esta teoría utiliza el marco general de la teoría de Matza de la delincuencia y deriva para explicar en qué medida esta se puede adaptar a la cibercriminalidad mediada por internet. Matza (1964) postuló que el delincuente se enfrenta a un dilema moral. Por un lado, conoce la validez de las normas y valores sociales convencionales, por otro, ha sucumbido a las tentaciones permisivas de la subcultura desviada. Matza propuso que la mayoría de jóvenes no se socializaba completamente en conductas delictivas, sino que terminaban involucrándose en conductas delincuenciales y no delincuenciales dependiendo de factores situacionales (Goldsmith y Brewer, 2015).

Es este estadio en particular al que Matza se refería como estar dentro de un estado de "deriva", o transformación entre conformidad y delincuencia, impulsado por factores situacionales que "aflojan" los controles sobre las decisiones y acciones (Goldsmith y Brewer, 2015).

La teoría de la deriva digital -*digital drift*- propuesta por Goldsmith y Brewer (2015) afirma que la teoría de Matza de la delincuencia y deriva es útil para entender entornos en línea donde ocurre ciberdelincuencia juvenil. Los autores enfatizan la idea que el “entrar y salir” de caminos criminales a menudo puede ser una decisión "accidental o impredecible". Es así que el Internet habría alterado fundamentalmente los arreglos sociales específicos para la comisión del delito, al permitir que los individuos actúen

solos y sin depender de coautores o entrenadores la mayoría de veces.

De acuerdo con Goldsmith y Brewer, el internet habría empoderado a los jóvenes a participar en prácticas de "recopilación de información asimétrica y no transparente", mediante la participación en comunidades virtuales, las que podrían incluir actividades criminales graves, es así que el acceso a internet facilitaría la exposición a entornos donde las influencias prosociales son menos efectivas.

Es así que:

> el coqueteo con nuevas identidades y el anonimato en línea, dada la relativa ausencia de guardianes capaces (…) liberaría a los jóvenes del sentido de responsabilidad, consiguiendo alentarlos o envalentonarlos a actuar de maneras que no lo harían en el mundo real. (Goldsmith y Brewer, 2015, p. 126)

En concordancia con Holt, Brewer, y Goldsmith (2019) en los entornos digitales se desarrollan características propias del espacio, muy distintas al espacio no virtual. De ahí se sigue que “en entornos digitales las autoridades tradicionales retroceden a un segundo plano mientras surgen nuevas influencias, a menudo transgresivas, fomentando así la desviación del grupo” (p. 1144). Según los autores los participantes jóvenes serían fácilmente atraídos a comunidades virtuales desviadas, para al cabo de un tiempo, en función de sentirse libres de las normas tradicionales mientras están en línea, elegirían volverse infractores por voluntad propia.

Una limitante de la teoría de la deriva digital es que a la fecha no hay estudio de investigación empírico que valide este marco conceptual. De poder existir estudios empíricos de casos concretos, los hallazgos servirían para explicar los procesos que argumentan los autores desencadenarían la deriva digital, o la también llamada participación juvenil en cibercrímenes en función de sentirse libre de las normas tradicionales mientras se está en línea. Sin embargo, se ha considerado útil incluirla en la medida que procura entender la disposición volitiva del demográfico juvenil, que termina adentrándose en el mundo del ciberdelito.

3. Teorías culturales

Estas teorías se enfocan en el contexto cultural del individuo para inferir como la conducta delictiva es moldeada por la influencia de componentes ligados al aprendizaje, la comunicación, obervación, e interacción a nivel microsocial, como relaciones

familiares y/o de pares, o macrosocial, como la estructura social, la localización diferencial, entre otros.

3.1 Teoría del aprendizaje social

Este modelo se basa en los estudios de Akers (1977), quien mostró que las personas aprenden y modelan su comportamiento cuando se reúnen cuatro requisitos. Los requisitos de la teoría del aprendizaje social son (Akers, Krohn, Lanza-Kaduce, y Radosevich, 1995):

- Imitación: el comportamiento social se adquiere tanto a través del condicionamiento directo, así como a través de la imitación o el modelado del comportamiento de los demás.

- Refuerzo diferencial: desplegar una conducta desviada que persiste en el tiempo se origina en las recompensas, o castigos del pasado, y del presente asociados a dicha conducta.

- Definiciones: las personas aprenden mediante la interacción con grupos importantes en sus vidas "definiciones evaluativas" que esencialmente son normas, actitudes y orientaciones de aquel comportamiento o conducta que se percibe como buena o mala. Cuantas más personas definan una determinada conducta como buena o sea una "definición positiva" o al menos como una "conducta justificada" o sea una "definición neutralizante" en lugar de una conducta indeseable "definición negativa", dicha conducta se realizará con mayor frecuencia.

- Asociaciones diferenciales: los principales efectos conductuales provienen de la interacción en, o , bajo la influencia de aquellos grupos que controlan las principales fuentes de reforzamiento y castigo de los individuos. Los más importantes de estos grupos suelen ser los de amistad entre pares, y la familia, pero pueden incluir escuelas, religión, y otros grupos.

Este enfoque integrador del aprendizaje se conoce como la teoría del aprendizaje social. Según Winfree, Bäckström y Mays (1994), esta teoría se ha utilizado para explicar ciertos tipos de ciberdelitos, como piratería digital y formas básicas de *hacking*.

Tabla 10
Estudios Asociación diferencial y definiciones favorables

Estudio	**Skinner y Fream (1997)**	**Holt, Burruss y Bossler (2010)**
Objetivo	Validar si la teoría del aprendizaje social propuesta por Akers es un marco conceptual apropiado para comprender el ciberdelito.	Utilizar técnicas de modelado de ecuaciones estructurales para examinar si el constructo del aprendizaje social propuesto por Akers, entendido como modelo de estructura y aprendizaje social podría explicar conductas de desviación cibercriminal, como: piratería de *software*, medios audiovisuales, pornografía, música y *hacking*
Metodología	Cuestionarios distribuidos a 581 alumnos universitarios para que proporcionen datos sobre su participación en cinco formas de ciberdelitos en el último mes, año pasado y toda la vida. Los participantes fueron seleccionados de varias facultades dentro de la universidad que tenían departamentos académicos con los niveles más altos de uso de computadoras y estudiantes con un amplio conocimiento de aplicaciones informáticas. El conjunto de datos se filtró mediante regresión múltiple.	Encuestas estudiantiles a alumnos de tres universidades públicas. El demográfico elegido se consideró una muestra apropiada y de alto riesgo para analizar las formas de desviación cibercriminal más frecuentes en poblaciones universitarias.
Conclusiones	Los resultados indicaron que las medidas de asociación diferencial, como la de tener amigos dedicados al *hacking*, fue el predictor más fuerte para cometer dichas conductas en los círculos sociales universitarios. Los hombres admitirieron haber cometido *hacking* más veces que mujeres.	Los resultados determinaron que tanto la asociación diferencial con pares desviados como las definiciones que promuevan vulnerar la ley están significativamente relacionadas con un aumento de la cibercriminalidad.

Fuente: Skinner y Fream, 1997, p. 499-515; Holt et al.,2010, p. 57-61. Elaboración propia

3.2 Teoría de la desconexión moral

Elaborada por Bandura en el año 1999, señala que mediante un "el uso de uno o varios mecanismos de desconexión moral, la conducta perjudicial por parte del infractor se reconstruye cognitivamente para aparentar menos perjudicial para sí mismo y los demás, y así justificar la acción" (Gutzwiller-Helfenfinger, 2015, p.194).

Según Gutzwiller-Helfenfinge (2015, p. 196):

> Bandura identifica cuatro estrategias generales y ocho mecanismos o prácticas subordinadas de desvinculación moral que se activan selectivamente para debilitar el control moral. Estas estrategias pueden operar sobre el comportamiento en sí mismo, el sentido de responsabilidad personal del individuo, los resultados del comportamiento o sobre los destinatarios del comportamiento (Bandura, 2001, 2002; Bandura et al., 1996; Paciello et al., 2008).

Estos ocho mecanismos o prácticas selectivas de desvinculación moral según Gómez y Narváez (2019) se caracterizan de la siguiente manera (p. 606):

- Justificación moral: Se valida para sí mismo la moralidad de una acción como inmoral o incorrecta.

- Comparación ventajosa: consiste en agrandar otras conductas inhumanas para que la propia conducta moralmente incorrecta parezca menos perjudicial o incluso benevolente.

- Lenguaje eufemístico: las acciones pueden tomar otra apariencia dependiendo de cómo se llamen, la persona hace uso de un lenguaje que modera y disminuye la importancia del comportamiento censurado.

- Desplazamiento de responsabilidad: ocultar o minimizar la conducta realizada a través de la atribución de la responsabilidad a otras personas o una autoridad legítima, en lugar de asumir responsabilidad por las acciones.

- Difusión de responsabilidad: cualquier daño hecho en grupo siempre puede ser atribuido en gran parte al comportamiento de otros, las personas actúan con mayor crueldad cuando existe responsabilidad grupal que cuando se hacen personalmente responsables de su conducta.

- Distorsión de consecuencias: los daños ocasionados por una conducta se ignoran, malinterpretan o minimizan, evitando que se active la autocensura moral.

- Deshumanización: se considera a la persona a la cual se le hace daño como carente de humanidad, salvaje, cruel o desalmada. La finalidad de despojarla de toda humanidad sirve para justificar el daño hacia ella.

- Atribución de culpa: los perpetradores se consideran a sí mismos como víctimas impulsadas a realizar la conducta perjudicial por una provocación forzosa, atribuyéndole la culpa a los demás.

A la luz de esta teoría los cibercriminales lograrían vencer su control moral interno o capacidad de autocensura, desconectándola de la conducta perjudicial sobre la víctima, mediante el empleo de los mecanismos cognitivos propuestos por Bandura. En consecuencia, de acuerdo con Rogers, Siegfried y Tidke (2006):

> la evidencia respalda que los cibercriminales reportan altas tasas de refuerzo diferencial, asociación diferencial y desconexión moral frente a los no delincuentes. También se cree que una combinación de estos tres (es decir, refuerzo diferencial, asociación diferencial y desconexión moral) predice mejor el comportamiento de un cibercriminal (p. 101).

En efecto, los estudios criminológicos han encontrado que la asociación y el refuerzo diferencial se correlacionan positivamente con ciertos tipos de comportamiento desviado, como son; drogas, delincuencia, abuso de alcohol, y conductas informáticas desviadas (Akers, 1977; Akers, 1998; Akers et al, 1979; Skinner y Fream, 1997).

Tabla 11
Estudio desconexión moral

Estudio	**Rogers (2001)**
Objetivo	Validar la hipótesis de trabajo que sugeiere que la combinación de asociación diferencial, refuerzo diferencial, y desvinculación o desconexión moral, predice mejor la cibercriminalidad que cualquiera de las variables por sí sola.
Metodología	Estudio de cuestionario de autoinforme de tres fases; la primera fase fue exploratoria y comparó variables sociodemográficas de ciberdelincuentes y delincuentes en general. El objetivo fue determinar si existen características exclusivas de cibercriminales en comparación con delincuentes en general. La segunda fase examinó las diferencias, si las hubiera, entre los ciberdelincuentes, los delincuentes generales y los no delincuentes en las variables de aprendizaje social y desconexión moral. La tercera fase, examinó la combinación de variables que proporcionaron el modelo más eficiente para predecir la ciberdelincuencia
Conclusiones	Los ciberdelincuentes exhiben tasas significativamente más altas de asociación y refuerzo diferencial en comparación con los no-ciberdelincuentes. Asimismo, los ciberdelincuentes tuvieron tasas significativamente más altas de desvinculación/desconexión moral que los participantes no-ciberdelincuentes. Por lo tanto, los *hackers* emplean mecanismos de desvinculación moral como medio para reducir la autocensura (Chantler, 1996; Denning, 1998; Parker, 1998). Asimismo, los *hackers* consideran su actividad como un pasatiempo puramente intelectual y consideran que la información debe estar disponible de manera gratuita para todos (Chantler, 1996; Taylor, 1997). Estos serían claros ejemplos de justificación moral (Rogers, 2001). Otros estudios han encontrado que los *hackers* minimizan o malinterpretan de manera rutinaria las consecuencias de *hacking* (Chantler, 1996; Parker, 1998; Rogers, 2001) Los *hackers* deshumanizan a sus víctimas y se refieren a ellas en términos tales como corporaciones multinacionales o redes y sistemas. El mecanismo más comúnmente exhibido es el de culpar a la víctima, así como a los administradores del sistema o programadores por la falta de seguridad, y declaran que bajo la ineptitud

	de los últimos, las víctimas habrían sido atacadas de manera eventual (Chantler et al., 1996). La evidencia establece que los *hackers* utilizan técnicas comunes de neutralización, negando que sus acciones causen daño a sus víctimas. (Gordon y Ma 2003; Morris, 2011), para así culparlas por no contar con buenas herramientas de seguridad o habilidades necesarias para prevenir la victimización (Jordan y Taylor, 1998; Taylor, 1999; Holt, Brewer y Goldsmith, 2019).

Fuente: Rogers, 2001, p.138-147. Elaboración propia

3.3 Teoría de las subculturas

Dentro de las teorías culturales o tambien llamadas del aprendizaje social se incluye la teoría de las subculturas, debido a que de acuerdo con Cohen (1955), esta guardaría componentes culturales y de aprendizaje social, en la medida que:

> la cultura está en una continua y constante creación, recreación, y modificación, donde los individuos perciben mutuamente necesidades similares, generadas por circunstancias similares, generalmente no compartidas en el sistema social más amplio, y, además, el actor social también está involucrado en un proceso continuo de realineación de grupos (p.11).

Es así que en *Delinquent Boys: The Culture of the Gang* (1955), Albert Cohen empieza definiendo cultura y subcultura del siguiente modo:

> [...] conocimiento, creencias, valores, códigos, gustos y prejuicios que son tradicionales en los grupos sociales y que se adquieren mediante la participación en dichos grupos (...) Cada sociedad se diferencia internamente en numerosos subgrupos, cada uno con formas de pensar y hacer que son en muchos aspectos particularmente propios, que uno puede adquirir solo participando en estos subgrupos y que apenas puede ayudar con la adquisición cuando ya se es un participante completamente integrado. Estas culturas dentro de las culturas son "subculturas". (1955, p.12)

De acuerdo con Yousry (2018) Cohen se diferenció de los sociólogos que lo antecedieron al hacer hincapié en los valores y la conducta, en lugar de la posición social para explicar la pertenencia del individuo a la subcultura, Cohen se centró en la noción de desviación como conducta y actitud aprendida.

Cohen señala que una determinada subcultura encuentra su propio nicho característico dentro de las estructuras sociales a través de ciertas geografías socioeconómicas, que posibilitan que florezca, en consecuencia es posible que en otros lugares dicha subcultura no pueda desarrollarse. La naturaleza de estas subculturas delincuenciales enfatiza lo que Cohen denomina autonomía de grupo, dentro de la cual habría valores como lealtad, solidaridad y alianzas presentes, que reemplazarían a todas las demás

relaciones (Yousry, 2018).

Según Cohen (1955), el consenso es decir, alguna forma de conformidad, no solo se ve recompensado por la aceptación, el reconocimiento y el respeto, sino que es probablemente el criterio más importante de validez del marco de referencia, que luego trabaja para motivar y justificar la conducta del actor social.

Así es como se forman y mantienen las subculturas delincuenciales, con la subcultura actuando como una solución a los problemas interpretados por los actores sociales. “La condición social crucial para el surgimiento de una nueva subcultura es la interacción efectiva de un número de actores sociales con "problemas de ajuste" similares” (Cohen, 1955, p. 35).

Cohen afirma que "La migración de individuos de un grupo a otro, de una cultura a otra es con frecuencia la búsqueda inconsciente de un entorno social favorable a la resolución de problemas de ajuste" (p. 58). Es así que para Cohen el mantenimiento continuo y la viabilidad de una solución subcultural, implica dos cosas:

> a) el surgimiento de una cierta cantidad de solidaridad grupal, y b) una mayor interacción entre los participantes de la subcultura. Es solo a través de la interacción con aquellos que comparten los mismos valores subculturales, que el actor social encuentra la validación de sus creencias, y recompensas sociales por su estilo de vida. (p. 72)

En consecuencia, sucede en muchos casos, que las subculturas, y específicamente las subculturas delincuenciales, representan un nuevo sistema de estatus que aprueba o autoriza el comportamiento etiquetado como prohibido o desaprobado por la cultura dominante (Yousry, 2018).

Tabla 12
Estudio de subcultura hacker

Estudio	**Holt (2005)**
Objetivo	Entender como el comportamiento individual es moldeado por normas subculturales y sistemas de valores, e informarse de las creencias, racionalizaciones, y conductas que profesan aquellos individuos que operan dentro de la subcultura hacker, tanto solos como en contextos grupales.
Metodología	Triangulación de datos a partir de 3 conjuntos de muestreos de miles de observaciones y encuestas realizadas en la convención de *hackers* más grande del mundo -Defcon-, foros y demás sitios *web* donde la organización social de la subcultura hacker opera. Los valores y normas subculturales se medirán utilizando el concepto de "orden normativo" de Herbert (1998).

Conclusiones	El mundo social de los *hackers* está conformado por cinco órdenes normativas, siendo estas: a) Tecnología, b) Conocimiento, c) Compromiso, d) Categorización, y e) Derecho. Las órdenes se utilizan para generar justificaciones con respecto a la conducta, medir el efecto sobre las actitudes hacia el *hacking* y estructurar la identidad y el estatus dentro de la subcultura. Tecnología: La conexión entre computadoras y tecnología tiene un rol clave en la estructuración de sus intereses y actividades (ver también Jordan y Taylor 1998; Taylor 1999; Thomas 2002). El nivel de conocimiento de un *hacker* se relaciona directamente con su capacidad y habilidad (véase también Thomas 2002: 44). Conocimiento: La identidad *hacker* se basa en una devoción por aprender y comprender tecnología. Desarrollar un amplio conocimiento de sistemas, *hardware*, programación y redes fueron consideradas habilidades extremadamente importantes, porque estas influyen directamente en el *hacking*. El aprendizaje y el conocimiento estan ligados al estatus y respeto dentro de la subcultura tanto en línea como fuera de línea. Compromiso: Es necesario una forma de compromiso para aprender temas que consideran interesantes en la intersección de las computadoras y la tecnología. Aunado a este compromiso, los cambios continuos y mejoras en la tecnología incrementan el tiempo requerido para aprender. Los *hackers* deben estar comprometidos con la identificación y adquisición continua de nueva información. La subcultura *hacker* le asigna un importante valor al compromiso constante de aprender a lo largo del tiempo. Categorización: Las diversas interpretaciones en torno a las ideologías de sombreros blancos (*white hats*) y negros (*black hats*) ilustra la importancia de la opinión individual del *hacker*. La forma que los individuos crean y definen la identidad del *hacker* constituye el cuarto orden normativo de la subcultura. Derecho: Este orden se reflejó en las discusiones sobre la legalidad del *hacking* e intercambio de información en el mundo fuera y dentro de línea. De los datos obtenidos, se confirmó que compartir "información ilegal" no fue tolerada, es decir sugerir a personas participar en "actividades delictivas", o dar acceso a materiales cuestionables, u obtenidos "ilegalmente" no es una práctica bienvenida en entornos públicos dentro, o fuera de línea. Sin embargo, compartir información que "podría" usarse de manera delictiva, si fue aceptable.

Fuente: Holt, 2005, p.61-211. Elaboración propia

4. Teorías de la oportunidad

Según Cox, Johnson y Richards (2009) las teorías de la oportunidad se han utilizado durante casi tres décadas para explicar de manera efectiva la causalidad en diversas categorías de delitos, y aún continúa sirviendo como base teórica de varias explicaciones prácticas de la conducta criminal contemporánea. Otros autores como Maras (2015), sostiene que el aporte de estas teorías no es contribuir a la solución de como "corregir" a los delincuentes, sino más bien de como corregir aquellos lugares y situaciones que posibilitan delinquir, para de esta manera bloquear dichas oportunidades.

4.1 Teoría de las actividades rutinarias

Esta teoría fue propuesta por Felson y Cohen (1979) también conocida como la teoría de las actividades cotidianas y se explica mediante la intersección de tres factores: (1) delincuentes motivados; (2) disponibilidad de blanco o víctimas adecuadas; y (3) la ausencia de guardianes capaces. Los investigadores han utilizado esta teoría para comprender la relación y, o interacción entre el criminal y la víctima (Cox et al., 2009).

De acuerdo a Maras (2015) y Yar (2005) las teorías de las actividades rutinarias ayudan a elaborar estrategias de prevención y reducción del ciberdelito, es así que cuando se aplica al cibercrimen, la comisión de este deja de ser menos atrayente para cibercriminales motivados. Para Miró (2011) muchas de las investigaciones criminológicas sobre el ciberdelito de la actualidad utilizan el *"approach"* de la oportunidad, propuesta por la teoría de las actividades cotidianas (TAC) de Cohen y Felson.

Para las teorías de las actividades rutinarias el delito se suscita con normalidad a lo largo del día si las condiciones para su comisión son las adecuadas. Dicho de otra manera, el enfasis recae en si existe o no la oportunidad para que un crimen pueda ser cometido. La teoría de las actividades rutinarias establece que deben confluir tres elementos indispensables para crear el contexto, o , escenario ideal para la comisión de delito. Estos son: delincuentes motivados, objetivos adecuados, y guardianes incapaces, con respecto a los últimos estos podrían estar ausentes o no ser lo suficientemente responsables para cumplir su rol.

Tabla 13
Estudios ciberacoso en línea y ciberataques puros

Autores y año	**Vakhitova, Reynald, y Townsley (2016)**	**Maimon, Kamerdze, Cukier, y Sobesto (2013)**
Objetivo	Comprobar en qué medida los modelos de exposición al estilo de vida y actividad rutinaria explican el riesgo de victimización personal en el ciberespacio. El estudio busco examinar la viabilidad de la teoría de la actividad rutinaria para predecir la victimización por ciberacoso en línea de personas de 18 a 30 años en los EE. UU., Finlandia, Alemania y el Reino Unido. Como tal, este estudio representa la primera aplicación de la teoría de las actividades cotidianas a	Utilizar la teoria de Felson y Cohen y la teoría de estilos de vida propuesta por Hindelang Gottfredson y Garofalo (1978), para explicar a qué hora se realizarían ataques informáticos (*computer-focused crime; exploits* informáticos, escaneos de puertos y ataques de denegación de servicio - DoS) a una red universitaria de computadoras durante los próximos meses, y de que países serían las direcciones IP de los autores de dichos ataques.

	los fenómenos en línea en un contexto internacional. Con dos objetivos delimitados para el análisis; primero, determinar qué tan bien la TAC explica las experiencias de victimización en el contexto en línea y segundo, si las asociaciones de victimización en línea fueron similares a nivel internacional.	
Metodología	El principal método de recopilación de datos utilizado fue encuestas de victimización en línea utilizando muestras de estudiantes universitarios. Los datos resultantes se analizaron mediante regresión múltiple o logística controlados por factores sociodemográficos, exposición al delincuente, idoneidad del objetivo y la ausencia de tutela.	Para examinar la hipótesis de investigación, se emplearon datos recopilados del IPS de una universidad pública, con relación al número de ciberataques experimentados por su red informática, su nivel de gravedad y origen entre los años 2007 y 2009. Un IPS es un dispositivo diseñado para monitorear el tráfico de una red informática con el fin de detectar y prevenir ciberataques e intrusiones a la red. Estos datos se cruzaron con los registros oficiales de la universidad. También se adjuntó información a nivel de país del Banco Mundial a los registros de análisis. Para el procesamiento de los resultados se empleó un modelo de regresión binomial negativa.
Conclusiones	Las experiencias de ciberacoso en línea fueron relativamente comunes en cada uno de los cuatro países, entre el 15 a 20 por ciento de la población encuestados. En términos de objetivo idóneo, la edad fue un factor de riesgo significativo en todos los países, excepto Finlandia, lo que indica que los usuarios más jóvenes tenían un riesgo significativamente mayor de victimización en los tres países. Esto está en línea con otros estudios realizados sobre victimización en línea, ya que los usuarios más jóvenes tienden a ser más activos de Internet y las redes sociales, por lo que corren un mayor riesgo de tener experiencias negativas.	Los hallazgos confirmaron que era más probable que los ataques ocurran durante el horario comercial de la universidad, debido a los picos de mayor tráfico de usuarios en la ausencia de un guardián capaz. Específicamente, y de acuerdo con la teoría y la investigación de la criminología que indican que el riesgo de victimización es particularmente alto durante los momentos del día en que es probable que se encuentren los delincuentes motivados y los objetivos adecuados. Esto aunado a la creciente tasa de usuarios extranjeros accediendo redes locales, como el intranet y demás bases de datos, multiplicarían las posibilidades del ciberataque. Es así que las tasas más altas de usuarios extranjeros de la red aumentan la cantidad de delitos informáticos lanzados desde los países de origen de estos usuarios extranjeros. Este estudio respalda el punto de vista que sugiere que la teoría de las actividades rutinarias podría implementarse en el contexto del ciberespacio, particularmente cuando se estudian redes informáticas específicas que tienen más probabilidades de estar activas durante momentos determinados del día.

Fuente: Vakhitova et al., 2005, p.11-16; Maimon et al., 2013, p.339-343. Elaboración propia

Tabla 14
Estudios víctimas de ciberacoso y desfiguraciones web

Autores y año	**Reyns, Henson y Fisher (2011)**	**Holt, Van Wilsem, Van de Weijer y Leukfeldt (2020)**
Objetivo	Se empleó la teoría de las actividades cotidianas y la base de las ideas de Eck y Clarke (2003) para explicar los crímenes en los que no hay contacto cara a cara entre las víctimas y delincuentes. Los autores desarrollaron una teoría adaptada de las TAC y la teoría de estilos de vida, para entender la victimización por ciberacoso en el ciberespacio. La finalidad del estudio fue realizar un análisis multivariado para identificar aquellos factores de riesgo que fomentan la victimización por ciberacoso.	Este estudio se valió de la teoría de la actividad rutinaria para explicar ciberataques contra sitios *web* holandeses mediante la modalidad de desfiguraciones *web*. El estudio buscaba medir la relación entre la visibilidad, inercia, valor y la accesibilidad del objetivo (Acrónimo VIVA empleado en la TAC) en espacios en línea con respecto a las motivaciones particulares no monetarias del atacante.
Metodología	Cuestionarios a víctimas universitarias de ciberacoso, los resultados se obtuvieron mediante análisis multivariante.	El estudio utilizó una muestra de 138,361 desfiguraciones *web* realizadas en sitios *web* alojados en el espacio IP de los Países Bajos desde enero de 2011 hasta abril de 2017. Con este fin se realizaron siete modelos de regresión logística multinomial por cada motivo identificado según el ataque, agrupados por cada atacante para minimizar el tamaño de errores estándar.
Conclusiones	Los hallazgos indicaron que la victimización por ciberacoso de universitarios se asocia con una serie de decisiones y comportamientos en línea que facilitan la intersección de la víctima y el delincuente. Específicamente, comportamientos que atraen a delincuentes motivados como; la proximidad virtual cercana con la víctima (es decir, agregar extraños como amigos a redes sociales), participar en actividades desviadas en línea (es decir, piratear contenido, acosar a otros) y asociarse con compañeros desviados en línea (lo que indicaría la ausencia de un "guardián capaz").	Los hallazgos demostraron que las consecuencias de los ataques son variadas y dependen en gran medida del objetivo y los intereses del actor. Los individuos tenían más probabilidades de afectar la página de inicio de un sitio cuando estaban motivados por un motivo ideológico o basado en desafíos, mientras que aquellos motivados por el deseo de divertirse, de ser considerados los mejores, por patriotismo, y por ninguna razón específica eran más propensos a desfigurar páginas secundarias. Esto puede ser un reflejo de la necesidad de afectar a un objetivo de alta visibilidad para demostrar habilidad técnica dentro de la subcultura *hacker* (Holt, 2007; Steinmetz, 2016) u obtener más testigos con respecto a la emisión de mensajes políticos. Los resultados refuerzan la hipótesis que las demostraciones de habilidad tecnológica son de gran importancia en la subcultura *hacker.*

Fuente: Reyns et al., 2011, p. 1149-1169 ; Holt et al., 2020, p. 187-206. Elaboración propia

4.2 Técnicas de prevención situacional del delito

Dentro del enfoque de las teorías de la oportunidad se sitúa las técnicas de prevención situacional del delito. Propuesta por Clarke (1997), que propone la manipulación de las condiciones del entorno que facilitarían el delito, con el objetivo de reducir las probabilidades para la comisión del mismo.

Según Summers (2009, p.396)

> las teorías en las que se basa las técnicas de prevención situacional del delito incluyen: la teoría de las actividades rutinarias (Cohen y Felson,1979); la teoría de la elección racional (Cornish y Clarke, 1986), la teoría del patrón delictivo (Brantingham y Brantingham, 1984, 1993); y aquellas teorías que enfatizan la modificación del ambiente físico para prevenir el delito, incluidas la prevención criminal basada en la modificación del ambiente físico (Jeffery, 1971), la teoría del espacio defendible (Newman, 1972); y, por último, la policía orientada a la solución de problemas (Goldstein, 1979).

Clarke (1997) sostiene que para prevenir el delito se debe modificar el entorno, aumentar los esfuerzos y riesgos involucrados, reducir potenciales recompensas, y dificultar el ataque para que el delincuente justifique su actividad con excusas.

Las técnicas de prevención situacional de delito se han utilizado para guiar esfuerzos preventivos en el ciberespacio en torno a delitos dentro del comercio electrónico (Newman y Clarke, 2013), amenazas de *insiders* o empleados cibercriminales (Siponen y Willison, 2009), robo de identidad (Copes y Vieraitis, 2009) y ciberacoso (Reyns, 2010). Cornish y Clarke (2003) propusieron cinco métodos que los guardianes podrían usar para proteger a las víctimas del delito: a) aumentar el esfuerzo, b) aumentar el riesgo, c) reducir ganancias, d) reducir provocaciones, y e) eliminar excusas.

Summers (2009, p. 397) detalla que las técnicas presentan características importantes que dificultarían la comisión del delito.

- Aumentar el esfuerzo persigue dificultar la comisión del ilícito (o por lo menos aparentar que lo es, ya que lo importante es la percepción del delincuente potencial). Esto se consigue mediante el entorpecimiento del objetivo, el control

de accesos y salidas, la desviación de transgresores y/o el control de los facilitadores del delito.

- Aumentar el riesgo busca hacer la detección del delito más probable. Esto se consigue mediante el aumento del número de guardianes, la facilitación de la vigilancia natural, la reducción del anonimato, la utilización de los "gestores" de sitios y/o el refuerzo de la vigilancia formal.

- Reducir ganancias percibidas del ilícito intenta reducir la rentabilidad (o expectativas) del delito. Esto se consigue al ocultar/eliminar/retirar objetivos, identificar la propiedad, interrumpir/trastornar los mercados delictivos y/o eliminar beneficios.

- Reducir provocaciones o disposiciones emocionales transitorias que motiven la comisión del delito. Esto se consigue al reducir frustraciones y estrés, evitar disputas, reducir la excitación emocional, neutralizar la presión del grupo de referencia y/o disuadir imitaciones.

- Eliminar las excusas se centran en aclarar las normas de conducta, incrementar los sentimientos de culpabilidad del infractor o facilitar la elección de opciones no delictivas. Esto se consigue al establecer reglas, fijar instrucciones, alertar la conciencia, incentivar la conformidad y/o controlar las drogas y el alcohol.

Tabla 15
Estudio ciberataques a dispositivos médicos

Autores y año	**Anandarajan y Malik (2018)**
Objetivo	*Internet of Medical Things* (IoMT), es el sistema conectado de dispositivos médicos y aplicaciones que recopila datos para transferirlos a las TICs de atención médica. Se utilizó esta teoría para identificar posibles amenazas de seguridad a los dispositivos de Internet de las cosas médicas (IoMT) y proponer mecanismos de control utilizando la teoría de prevención situacional del delito para reducir la probabilidad y el impacto de tales amenazas.
Metodología	Análisis predictivo a partir de estudios sobre dispositivos médicos (IoMT), redes, e incidentes relacionados a ciberataques situados en el sistema de salud estadounidense.
Conclusiones	Siguiendo las cinco categorías propuestas por Clarke se aplicó los hallazgos al contexto de IoMT de la siguiente manera:

	a) Aumentar el esfuerzo: se incluyeron estrategias diseñadas para hacer que el ataque sea más difícil de llevar a cabo. ej. la creación de barreras físicas entre el atacante y el dispositivo médico, como la encriptación y cifrado de los datos enviados desde el dispositivo médico a través de múltiples capas de seguridad, para hacer menos probable que el *hacker* pueda traducir los datos en cada una de las transferencias. b) Aumentar el riesgo: se incluyeron estrategias para que el *hacker* asuma que el riesgo era mayor que el beneficio. ej. fomentar que dos médicos en vez de uno analicen los datos del dispositivo IoMT para verificar la privacidad de los datos. c) Reducir ganancias: se incluyeron estrategias para disminuir la recompensa percibida por atacar un dispositivo médico. ej. se enviaron los datos a la nube en vez de almacenarlos en el dispositivo médico del paciente, creando así más barreras de entrada, además de bloquear el acceso al dispositivo físico. d) Reducir provocaciones: se incluyeron estrategias como hacer que el dispositivo IoMT sea más fácil de usar para los pacientes. ej. se concluyó que la reducción de la frustración y el estrés para los pacientes que usan dispositivos IoMT promovería el buen mantenimiento del dispositivo. e) Eliminar excusas: se incluyeron estrategias para evitar que el *hacker* malinterprete las regulaciones que rigen el uso de dispositivos médicos. ej; la configuración de reglas, procedimientos y marcos fijos frente a la actividad cibercriminal.

Fuente: Anandarajan y Malik (2018), p. 1-24. Elaboración propia

5. Conclusiones

- La cibercriminalidad pura adopta una explicación multifactorial, en la medida que ninguna de las teorías propuestas permite explicarla a partir de una causa única, sino de un "paquete" de condiciones interrelacionadas de aplicabilidad variable.

- Dentro de las teorías de control; se propuso la teoría del autocontrol, la de vínculos sociales, y la de deriva digital. La primera establece que los individuos con escaso autocontrol tienden a piratear contenido digitalmente además de realizar formas básicas de *hacking*. La segunda corrobora que aquellos individuos con vínculos sociales como la supervisión parental e interés académico fueron menos proclives a participar de *hacking*. La tercera indica que la población juvenil participaría en cibercrímenes en función de sentirse libre de las normas tradicionales mientras están en línea detrás del anonimato.

- Dentro de las teorías culturales; se propuso la teoría del aprendizaje social, la desconexión moral, y la de subculturas. La primera establece que tanto la asociación diferencial con pares desviados como las definiciones favorables a la

violación de la ley están significativamente relacionadas con un aumento de la cibercriminalidad. La segunda demuestra que los cibercriminales tienen tasas más altas de desconexión moral en comparación con grupos no cibercriminales. La tercera sostiene que el mundo social de los *hackers* es una subcultura conformada por cinco órdenes normativas.

- Dentro de las teorías de la oportunidad; se propuso la teoría de las actividades rutinarias, y las técnicas de prevención situacional. La primera plantea que ciertas conductas atraen a delincuentes motivados como; la proximidad virtual, la participación y asociación con pares desviados en línea. La segunda confirma que mediante cinco técnicas situacionales los guardianes capaces podrían proteger a potenciales víctimas de ser el blanco de un ciberataque.

- De acuerdo con la evidencia mostrada, la etiología del cibercrimen debe entenderse de manera holística por las siguientes razones. Primero, de acuerdo con los profesores Back y LaPrade (2019) solo a través de un enfoque holístico es cuando el comportamiento de las personas, y la acción preventiva son tan importantes como implementar estructuras sólidas de ciberseguridad para mitigar de manera eficaz las ciber amenazas.

- Segundo, de acuerdo con Bjørgo (2016) y Sorsby (2018) en lugar que los modelos actuales de prevención de delito como pueden ser el modelo de justicia penal, el modelo social, el modelo situacional y/o modelo de gestión de riesgos, sean meramente enfoques incongruentes o competitivos, se recomienda complementarlos para que solo así se puedan fortalecer de manera conjunta, de esta manera al unificar los mecanismos de prevención, la estrategia integral debe basarse en incorporar una valla de barreras que operen juntas o de manera holística.

- Es evidente que el modelo integral de prevención de delito propuesto por Bjørgo se complementaría mejor de operar de manera integrada, en vez de desplegarse como unidades subdivididas y desligadas unas de otras. El problema radica en que al tratar a estos modelos preventivos como si fueran mecanismos individualizados, se estaría aceptando la premisa errada de creer que no comparten una finalidad en común: la lucha contra el cibercrimen.

- En consecuencia, tanto para Bjørgo (2016) como para Back y LaPrade (2019) el funcionamiento de un modelo sinérgico de prevención del delito debe tener un fuerte y necesario enfoque holístico. Bajo este símil, las operacionalizaciones de las teorías criminológicas deben entenderse holísticamente en la medida que se pueda utilizar los componentes generales de todas y aquellos particulares de algunas para avanzar el entendimiento existente sobre las causas y motivaciones que originan la conducta cibercriminal.

- Finalmente, la evidencia empírica mostrada en este capítulo es recomendable utilizarla de manera complementaria bajo el mismo enfoque holístico propuesto por los autores mencionados, porque solo a través de este enfoque se podrá entender de manera adecuada la suma de los hallazgos empíricos en su relación con la prevención y lucha contra la cibercriminalidad.

Los estudios criminológicos propuestos sirven de soporte teórico para implementar políticas criminales eficientes que prevengan y combatan la cibercriminalidad. En el siguiente capítulo se explorará la experiencia comparada de actores estatales en distintas regiones para identificar las medidas de intervención realizadas, o por realizar, con la finalidad de combatir y prevenir la cibercriminalidad.

CAPÍTULO 3

Política criminal y Cibercriminalidad Pura: experiencia comparada

1. Experiencias comparadas en torno a la prevención

En muchos países los agentes estatales han adoptado diversas políticas de prevención del cibercrimen. En este sentido, el estado es el agente más idóneo en términos de credibilidad y legitimidad, además de contar con los recursos necesarios para garantizar que existan medidas adecuadas de ciberseguridad que protejan a sus ciudadanos y organizaciones de amenazas cibercriminales (Kshetri & Kshetri, 2016)

Como sostiene Kshetri & Kshetri (2016) en el frente de la alta tecnología, el desarrollo de capacidades en caso de una guerra informática ha sido una tendencia notable en los últimos años. Es así como, hace exactamente diez años un artículo de *The Economist* pronosticó "Después de la tierra, el mar, el aire y el espacio, la guerra ha entrado en el quinto dominio: el ciberespacio "(p. 7).

En esta línea, Nye (2013) resaltó que, en el año 2013, veinte naciones contaban con unidades militares dedicadas a la guerra informática. Esto es coherente en la medida que, según Klimberg (2012), "contar con una estrategia de ciberseguridad ha sido un componente clave dentro de los marcos de seguridad nacional de las naciones miembros de la OTAN" (p. 44). En este orden de ideas, el Centro de Excelencia Cooperativo de Defensa Cibernética de la OTAN señala que, "desde el 2012, más de 50 países han promulgado una estrategia de Ciberseguridad en aras de combatir la cibercriminalidad" (Klimberg 2012, p. 46).

A continuación, se presentará tablas de información sobre diversos marcos institucionales, reglamentos, estándares, y estrategias de ciberseguridad implementados a través de regulaciones estatales que posibilitan a ciertos países y continentes hacerle frente al fenómeno de la cibercriminalidad.

1.1 América del Norte

Marcos legales sobre cibercrimen en Estados Unidos entre los años 1977 y 2015.

Tabla 16
Estados Unidos

Año	Marcos Legales y Regulatorios
1977	Ley Federal de Protección de Sistemas Informáticos.
1984	Ley de abuso y fraude informático (primera pieza de legislación centrada en el cibercrimen).
1985	A partir de 1985 las regulaciones sobre ciberseguridad incluyó a las instituciones financieras, como la banca, los seguros y las inversiones, junto con terceras partes o entidades que procesaban o recibían información de dichas instituciones.
1996	Ley de Responsabilidad y Portabilidad de Seguros de Salud, denominada HIPAA (*The Health Insurance Portability and Accounting Act*).
2002	La siguiente legislación sobre ciberseguridad cubrió a las agencias federales, a través de la ley Federal de Gestión de Seguridad de la Información (FISMA).
2005-2015	Ley Nacional de ciberseguridad (*The Cyber Act*), Ley Federal de Modernización de la Seguridad de la Información, Ley de Evaluación de la Fuerza Laboral de ciberseguridad, Ley de Evaluación de la Fuerza Laboral de Seguridad Nacional y la Ley de Mejora de la ciberseguridad.

Fuente: Wang (2016, p. 99-127), Bayard (2019, p. 71-94), Conrad (2018, p. 296-323), Brandon (2014, p. 22), y Wolf (2018, p. 789). Elaboración propia.

A la fecha todos los estados federales tienen una legislación que impone a las empresas el deber de revelar cuando se violan los datos personales de sus clientes (*data breach*). A nivel estatal se han introducido marcos de ciberseguridad para instituciones específicas, como las instituciones financieras, debido a los potenciales riesgos de ciberataques.

De acuerdo a Wolf (2018) La estrategia de ciberseguridad estadounidense está impulsada por visiones y prioridades distintas en comparación con la de la Unión Europea. Esta hace hincapié en la lucha contra las ciber-amenazas mediante ciber-operaciones, y unidades especializadas de investigación y prevención, no necesariamente en un marco basado en principios que proporciona un modelo para las buenas prácticas. Por esta razón la estrategia de ciberseguridad estadounidense es regulada bajo requerimientos específicos de las industrias.

La política cibercriminal estadounidense se encuentra muy desarrollada, por ser pionera en la materia, y tener la legislación más completa al respecto, según la literatura especializada cuenta con múltiples estrategias preventivas del delito, así como enfoques de prevención primaria, secundaria, y terciaria según el estado federal y el contexto en el tiempo bajo análisis, además de regulaciones sectoriales, y mecanismos hechos a medida para combatir la cibercriminalidad pura y demás vertientes.

Por ejemplo, el estado de California en el año 2021 publicó -Cal-Secure-, descrito como el itinerario de los próximos años del estado hacia la madurez digital en materia de

ciberseguridad. Este documento gubernamental planea sustanciales iniciativas que involucra la conjunta participación del sector público y privado, además de personas, procesos y tecnología, con la finalidad de beneficiar a los residentes y al gobierno federal.

Dado que este enfoque impulsado por el gobierno federal, necesita los aportes del sector público y privado para llevarse a cabo de manera eficiente, se observa en acción una respuesta de tipo co-regulatorio -*top-down*-, propuesta por Tropina y Callanan, y respaldada por Sales, debido a que soluciones de esta naturaleza como se dijo requieren la intervención y observancia estatal como componente necesario para su implementación.

Por ende, como lo autores señalaron resultaría en un error por parte del sector público, en este caso el gobierno federal descuidar la importancia de consolidar una sinergia con el sector privado, en la medida que el papel fundamental del gobierno es la de desempeñar liderazgo de la seguridad en el ciberespacio.

1.2 Europa

Marcos legales sobre cibercrimen en la Comunidad Europea entre los años 2001 y 2020.

Tabla 17
Europa

Año	Marcos Legales y Regulatorios
2001-2004	Resultado de más de una década y media de trabajo preparatorio, el Convenio del Consejo de Europa sobre el ciberdelito fue el primer instrumento multilateral vinculante para regular el ciberdelito. La Convención se abrió a la firma el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004.
2013-2017	Las instituciones de la UE refuerzan la cooperación para combatir los ciberataques. Por medio de un acuerdo interinstitucional se crea un Equipo de Respuesta a Emergencias Informáticas (CERT-UE), de carácter permanente, que cubre todas las instituciones, órganos y organismos de la UE.
2018	El Consejo Europeo pide medidas para fortalecer la ciberseguridad en la UE. Para lograr ese objetivo, el Consejo adopta una versión actualizada del marco político de ciberdefensa de la UE, y aprueba la propuesta de Reglamento sobre la Ciberseguridad, lo que permitirá que la Unión Europea introduzca una certificación de la ciberseguridad a escala de la UE y consolide una agencia permanente de la UE para la ciberseguridad.
2019	El Consejo adopta el denominado Reglamento sobre la Ciberseguridad, que introduce: un sistema de esquemas de certificación a escala de la UE, y una Agencia de la UE para la Ciberseguridad a fin de sustituir a la actual Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA), también establece un marco que permite a la UE imponer medidas restrictivas específicas para impedir los ciberataques que constituyen una amenaza externa para la UE o sus Estados miembros y responder a ellos

2020	En Julio la UE impone por primera vez sanciones en respuesta a ciberataques

Fuente: consilium.europa.eu (2020), Kshetri y Kshetri (2016, p. 108-128), Westby (2019), Clough (2014, p. 651). Elaboración propia.

En el año 2020 otra de las iniciativas de la Comunidad Europea contra la prevención del cibercrimen, fue la publicación de un plan de estrategia de ciberseguridad denominado "Un ciberespacio abierto, seguro y protegido", de manera conjunta con una directiva sobre seguridad de las redes y la información, ambas estrategias representan la visión integral de la UE sobre cómo prevenir, y responder de manera pronta y adecuada, posibles contingencias, disrupciones y ciberataques.

Las economías de la UE se han dado cuenta de la necesidad de competencias básicas en preparación y respuesta ante ciber-desastres. Es así que La Agencia Europea de Seguridad de las Redes y de la Información -ENISA- organizó el ejercicio de ciberseguridad más grande y complejo de Europa: Cyber Europe 2014.

Otra campaña de ejercicios de fortalecimiento de capacidades con la participación de los países miembros se llevó a cabo en el 2015 y 2016 respectivamente, cuando ENISA anunció el plan de llevar a cabo más de 2000 ciber-incidentes separados, que incluían ataques de denegación de servicio (*DoS*) a servicios en línea y ataques a infraestructuras críticas.

Como se puede observar la UE ha fortalecido sus capacidades de ciberseguridad y ciberdefensa mediante diversas campañas de ejercicios de preparación, y respuestas ante ciberamenazas. Enfoques de prevención del delito de este tipo son de corte secundario en la medida que toman lugar donde el delito se exterioriza, ya sea mediante potenciales ataques diseñados para incrementar las competencias de ciberdefensa y ciberseguridad, o mediante la implementación de estrategias de ciberseguridad que buscan prevenir, y responder mejor a disrupciones y ciberataques.

1.3 Asia

Marcos legales sobre cibercrimen en la República Popular de China entre los años 2005 y 2018.

Tabla 18
China

Año	Marcos Legales y Regulatorios
2005-2007	Los delitos informáticos en China se abordan mediante una serie de instrumentos principalmente en tres niveles, el primero es: a) La Ley Penal emitida por la Asamblea Popular Nacional (APN), y las Enmiendas a la Ley y Decisiones Penales emitidas por el Comité Permanente de la APN. b) b) Los reglamentos administrativos emitidos por el Consejo de Estado (CS) y reglamentos departamentales emitidos por los Ministerios. c) Las interpretaciones judiciales emitidas por la Corte suprema del pueblo y la fiscalía general del pueblo.
2016-2017	El Comité Permanente de la Asamblea Popular Nacional de China aprobó la Ley de Ciberseguridad en noviembre de 2016, y entró en vigor en junio de 2017. Esta legislación es la primera ley de carácter integral a nivel nacional que busca abordar las cuestiones relevantes asociadas con la ciberseguridad.
2018	La Ley de Ciberseguridad, así como las demás leyes promulgadas a partir del 2018 en adelante reafirman el reclamo de China sobre la soberanía del ciberespacio, y esto, para algunos observadores occidentales, permite a China "legitimar el control autoritario" sobre el ciberespacio. La Ley de Ciberseguridad China, incluye: a) Las obligaciones legales de la red de operadores. Como resultado, las autoridades reguladoras tienen más monitoreo, investigación y poderes de ejecución. b) La defensa de infraestructura crítica: Si bien la ley dicta que el Consejo de Estado define el alcance específico y las medidas de protección de seguridad de la infraestructura de información crítica, se ha expresado la preocupación sobre la amplitud de estas facultades. c) El requerimiento de la localización de datos: La "localización de datos" generalmente se refiere a políticas que requieren que las empresas almacenen datos sobre los usuarios, pero solo en servidores dentro de las fronteras jurisdiccionales. d) Certificación, inspección y revisión de seguridad: China elaboró un conjunto de normas de ciber-seguridad en el 20017 en el Reglamento sobre protección clasificada de la seguridad de la información, que se conoce como el Esquema de protección de niveles múltiples ("MLPS"). e) La protección de información personal: La Ley de Ciberseguridad brinda a los ciudadanos una cantidad de protección sin precedentes para garantizar la privacidad de sus datos.

Fuente: Wang (2016, p. 84- 119), Lee (2018, p. 54-61), Lindsay (2015, p. 12), Hurwitz (2017), Keally (2017), Shackelford, Russell y Kuehn (2017), y Mitchell y Hepburn (2017), Xinhua (2019). Elaboración propia.

De acuerdo a Malekos (2022) China es el líder mundial en prácticas de vigilancia y censura, un ejemplo de esto es como Beijing utiliza tecnología de vigilancia masiva en la región autónoma de Uigur de Xinjiang para monitorear a la población y atacar a los musulmanes turcos. Además, se le considera un actor estatal con capacidad y recursos de lanzar ciberataques formidables que interrumpan, o paralicen servicios de infraestructura critica a nivel internacional.

Dado su estatus de ciber potencia, se presume que China debe contar con alguna política criminal destinada a prevenir y combatir el cibercrimen doméstico, así como internacional. Se observa que un ejemplo de esta política es la ley de ciberseguridad del 2018, que en línea generales según la prensa internacional, es un mecanismo de coerción legal para "legitimar el control autoritario" sobre el ciberespacio.

Se infiere que el partido comunista chino utiliza el aparato legal para avanzar la agenda política del gobierno, por lo tanto, es posible que exista una omnipresente e invasiva intervención estatal en cualquier enfoque preventivo del delito o estrategia que combata la cibercriminalidad, sin embargo, no se cuenta con información disponible debido al secretismo de la materia por parte del gobierno, que permita entender bajo que forma, o de que manera el partido comunista chino ejecuta su política cibercriminal.

1.4 Europa del Este

Marcos legales sobre cibercrimen en Rusia entre los años 1999 y 2020.

Tabla 19
Rusia

Año	Marcos Legales y Regulatorios
1999-2000	Según la Doctrina de Seguridad de la Información de Rusia, adoptada a finales de los años noventa, la seguridad de la información se define como "el estado de protección de sus intereses nacionales en la esfera de la información definida por la totalidad de los intereses equilibrados del individuo, la sociedad y el estado". Un propósito real detrás de esto es posiblemente aumentar la capacidad y legitimidad del estado para el ciber-control y la censura. Sin embargo, Rusia no quiere ser percibida internacionalmente como un país políticamente represivo.
2010-2015	Según la ley rusa de contenido en línea, que entró en vigor el 1 de agosto de 2014, todos los "organizadores de la difusión de información a través de Internet" deben registrarse en Roskomnadzor y almacenar información sobre los usuarios y mensajes electrónicos durante 6 meses. La información debe proporcionarse a solicitud de los investigadores gubernamentales y las autoridades policiales.
2019	La cámara baja del parlamento de Rusia, la Duma, aprobó a finales del 2019 una legislación que proporcionaría un "funcionamiento sostenible" del Internet en Rusia, en caso que el país estuviera desconectado del resto de la red global.
2020	Al igual que China, espera aislarse del Internet global y ha tomado medidas enérgicas contra el uso de VPNs (*Virtual Private Networks*), mediante una Ley que obliga a los proveedores de servicios de Internet a instalar equipos especiales que puedan rastrear, filtrar y desviar el tráfico de Internet. Esta maquinaria tecnológica permite al regulador de telecomunicaciones ruso, Roskomnadzor, bloquear de forma independiente y extrajudicial el acceso al contenido que el gobierno considera una amenaza.

Fuente: Thomas (2001, p. 313), Boiten (2014), Gulyaeva y Sedykh (2014, p. 129-139), Weber (2020), Rodgers (2019), Schulze (2019), hrw.org (2020). Elaboración propia.

Es a partir del 2012 que Rusia experimentó protestas antigubernamentales a gran escala que exigían una reforma política radical, por esta razón gradualmente ha adoptado medidas que se asemejan mucho al enfoque de China para el control de la información.

En los años posteriores, ha pasado de la censura general al despliegue de métodos sofisticados como "la inspección profunda de paquetes" -*Deep Packet Inspection*-, que hacen de la censura una herramienta con mayor precisión. Putin ha tomado una serie de pasos para frenar las libertades en línea, como por ejemplo prohibir el servicio de mensajería encriptada Telegram, sin embargo, muchos de esos intentos han resultado infructuosos.

En su momento fue de conocimiento público que Rusia venía preparándose tecnológicamente en caso iniciará una guerra, y como resultado occidente le corte el acceso a internet, pero al igual que el secretismo en China con respecto a la política cibercriminal empleada en vigencia, el gobierno ruso tampoco ha revelado a medios extranjeros en que consiste su paquete normativo, iniciativas, o regulaciones destinadas para combatir y prevenir la cibercriminalidad. Por lo que no es posible inferir las herramientas que podría utilizar para dicho fin.

1.5 Oriente Medio

Marcos legales sobre cibercrimen en el Estado de Israel entre los años 2015 y 2016.

Tabla 20
Israel

Año	Marcos Legales y Regulatorios
2015-2016	Acuerdo Gubernativo N° 2444 de 15 de febrero de 2015, marcó el comienzo oficial de la Autoridad Nacional de Defensa Cibernética ("la Autoridad"). La finalidad del acuerdo fue “dirigir, operar y ejecutar, según sea necesario, todos los esfuerzos defensivos y operativos a nivel nacional en el ciberespacio, con base en un enfoque sistémico, para permitir una respuesta defensiva completa y constante a los ciberataques, incluido el manejo de las amenazas del ciberespacio y ciber eventos en tiempo real, formulación de una evaluación de la situación actual, recolección e investigación de inteligencia, y trabajo con las instituciones especiales.

Fuente: Even, Siman-Tov y Siboni (2016, p. 12-19), Leitersdorf y Schreiber (2019), Press (2017), Elaboración propia.

Israel se ha convertido en una potencia de ciberseguridad, como parte de su estrategia ayuda a naciones más pequeñas, como por ejemplo, Singapur, en esta línea ha creado más de 300 nuevas empresas de ciberseguridad, el año pasado exportó más de 6.5

miles millones de dólares en productos de ciberseguridad, convenció a más de 30 multinacionales para que abran centros locales de I + D en su territorio, y atrajo inversores extranjeros (Leitersdorf y Schreiber, 2019).

De acuerdo a los expertos serían seis factores clave que habrán contribuido al ascenso meteórico de Israel como un centro global para la investigación, y la práctica de la ciberseguridad. Estos son haber conseguido que el gobierno 1) opere como coordinador y 2) catalizador empresarial, 3) hacer del ejército una incubadora y aceleradora de nuevas empresas, 4) invertir en capital humano, 5) adoptar la interdisciplinariedad y la diversidad, y 6) repensar la "cibercaja".

Como se observa al igual en el caso de Estados Unidos, Israel ha logrado una sinérgica y provechosa relación entre el sector público y privado, posibilitando un enfoque co-regulatorio de asociaciones público-privadas, mediante la participación del ejército en el rol de incubadora y aceleradora de empresas tecnológicas.

1.6 Asia Oriental

Marcos legales sobre cibercrimen en Corea del Sur entre los años 2010 y 2020.

Tabla 21
Corea del Sur

Año	Marcos Legales y Regulatorios
2010-2015	En los últimos años, Corea del Sur ha introducido una serie de marcos legales, regulatorios y organizativos para hacer frente a las ciber-amenazas. En 2010, Corea del Sur desarrolló e implementó una ciber-estrategia. La primera parte del plan, que estaba en funcionamiento a principios de 2014, se centró en la protección de redes (Keck 2014). Antes de esto, ya se había establecido un ciber-comando en enero de 2010 y un equipo de políticas de ciber-protección redactadas por el SKDM -*South Korean Democracy Movement*- (Kshetri y Kshetri, 2016). El SKDM también estableció un Departamento de ciber-política en 2013. Un año después El NIS -*National Intelligence Service*- anunció que su tercer departamento prestaría mayor atención al monitoreo del ciberespacio y las telecomunicaciones (Kshetri y Kshetri, 2016).
2017-2020	De acuerdo con Lee y Ko, en Corea del Sur, las leyes aplicables a la ciberseguridad incluyen: la Ley de Redes, la Ley de Protección del Secreto de la Comunicación, la Ley de Gobierno Electrónico, la Ley de Establecimiento de Infraestructura para la Informatización de la Defensa Nacional, la Ley de Protección y Uso de la Información Crediticia, la Ley de Protección del Uso de la Información de Ubicación, la Ley de Prevención de Divulgaciones y Protección de Tecnología Industrial, y la Ley Especial de Fraude Financiero (iclg.com 2020).

Fuente: Kshetri y Kshetri (2016, p. 176), Keck (2014), National Security Office (2019). Elaboración propia.

La estrategia nacional de ciberseguridad del 2019 de Corea del Sur señala las siguientes seis tareas estratégicas para realizar en los próximos años (National Security Office, 2019): 1) incrementar la seguridad de la infraestructura central nacional, 2) mejorar las capacidades de respuesta a ciberataques, 3) establecer una gobernanza basada en la confianza y la cooperación, 4) sentar las bases para el crecimiento de la industria de la ciberseguridad, 5) fomentar una cultura de ciberseguridad, 6) liderar la cooperación internacional en ciberseguridad.

Como se observa en la estrategia nacional se revela que el gobierno desplegara un catálogo de medidas de prevención cibercriminal, en aras de fortalecer las capacidades de la industria de ciberseguridad, asimismo menciona enfatizar la cooperación de los distintos sectores que están relacionados con la ciberseguridad.

Marcos legales sobre cibercrimen en el Estado de Japón entre los años 2010 y 2016.

Tabla 22
Japón

Año	Marcos Legales y Regulatorios
2006	La Primera Estrategia Nacional de Seguridad de la Información (FSIS), promulgada en 2006, representó el primer intento de Japón de abordar el problema de la ciberseguridad a nivel nacional.
2010-2015	Siguiendo las recomendaciones del Centro Nacional de Seguridad de la Información (NISC), el Consejo de Políticas de Seguridad de la Información (ISPC) adoptó la Política para Mejorar la ciberseguridad japonesa y se transformó en la Sede de la Estrategia de Seguridad Cibernética (CSSH), responsable de crear la nueva Estrategia de ciberseguridad nacional de septiembre de 2015.
2016	La Ley Básica de ciberseguridad otorgó poderes mucho más completos para evitar que continúen las fallas al hacer una de sus misiones principales bajo la primera disposición de la Política General de la ley "el aseguramiento de la ciberseguridad en los órganos administrativos nacionales", bajo esta ley, un Operador de "data" debe tomar las medidas necesarias y apropiadas para el control de seguridad de los Datos Personales que maneja, incluida la prevención de la fuga, pérdida o daño.

Fuente: Shackelford, Russell y Haut (2016), Kallender y Hughes (2017), Hamada y Matsumoto (2019). Elaboración propia.

Japón proporciona protecciones básicas de privacidad y exige que los controladores de datos desplieguen mecanismos de respuesta adecuados para prevenir fugas, pérdidas o daños; y para monitorear mejor la seguridad de los datos personales, asimismo es importante señalar que se deja la implementación de estas leyes a agencias específicas del sector o también llamadas "multisectoriales", de las cuales hay veintisiete.

A modo de ejemplo, en la industria de sistemas de transporte inteligentes, la estrategia

vigente reconoce que debido a que la industria involucra a numerosos fabricantes, agencias gubernamentales, y sectores académicos, estos organismos en calidad de partes interesadas, deben unirse para desarrollar de manera conjunta estándares apropiados por los cuales se responsabilizarán.

Esto reafirma el compromiso de Japón con un enfoque colaborativo de abajo hacia arriba -*bottom up approach*- dentro de la política de ciberseguridad. En este sentido si bien la estrategia de auto-organización anticipa que el gobierno asumirá un papel de liderazgo en áreas de considerable importancia, a través de la Sede Estratégica de Ciberseguridad, el enfoque general de las industrias sigue siendo el autogobierno (Hamada y Matsumoto, 2019).

Como se observa la política cibercriminal japonesa incentiva la participación voluntaria del sector privado de abajo hacia arriba -*bottom up approach*-, también conocida por Tropina y Callanan como estrategias de "autonomía" y "autogobierno".

1.7 América del Sur

Marcos legales sobre cibercrimen en Brasil entre los años 2000 y 2020.

Tabla 23
Brasil

Año	Marcos Legales y Regulatorios
2000	Se creó la Política de Seguridad de la Información y el Comité Directivo de Seguridad de la Información (CGSI)). El cual incluía el mandato de establecer directrices, principios y objetivos para el desarrollo de normas, tecnologías nacionales y la preparación de las entidades y agencias de la Administración Pública Federal en el campo de la seguridad de la información.
2008	La Estrategia de Defensa Nacional (END), fue el primer documento oficial en reconocer el ciberespacio como uno de los dominios estratégicos para la seguridad y defensa nacional, marcando así la inclusión oficial de la ciberseguridad en la agenda de seguridad nacional.
2013	La aprobación del Marco Civil de Internet (la Carta de Derechos Digital) motivada por el impacto político de las revelaciones sobre la estructura de vigilancia virtual de Estados Unidos.
2014-2016	Incluyeron esfuerzos como (i) la creación del Centro de Ciberdefensa (CDCiber); (ii) esfuerzos de desarrollo de capacidades en ciberseguridad por parte de instituciones públicas a nivel federal y municipal; (iii) la mayor colaboración entre el gobierno y el sector privado; y (iv) el establecimiento de doctrinas, políticas y directrices relacionadas con la ciberseguridad.
2017	Se estableció el Comando de Defensa Cibernética (ComDCiber) y, lo más importante, integrado por representantes de todas las fuerzas armadas. La agencia es actualmente responsable de “planificar, orientar y controlar las actividades operativas, doctrinales de desarrollo y preparación a nivel del Sistema de Ciberdefensa Militar”

2020	Se publicó el Decreto Federal N° 10.222102 aprobando la Estrategia Nacional de Ciberseguridad (el Decreto). Más específicamente, este busca guiar a Brasil en la seguridad cibernética e incluye acciones para aumentar su resistencia frente a amenazas cibernéticas y fortalecer su desempeño a nivel internacional.

Fuente: Chatin (2016), Hurel y Lobato (2018), BID y OEA (2020, p. 70-76). Elaboración propia.

En Brasil las instituciones estatales se someten a evaluaciones de ciber-riesgo de manera anual, además de actualizarse en torno a la experiencia adquirida a partir de incidentes previos. El CERT nacional es la institución responsable de administrar reportes de incidentes y abordar los incidentes de ciberseguridad.

De acuerdo a Hurel (2019) si bien el gobierno ha estado desarrollando políticas nacionales y por sector industrial, así como en el caso de Estados Unidos, las leyes y regulaciones apenas se habían enfocado en la seguridad y privacidad de la data hasta recientemente. En esta línea en el año 2018 el Consejo Nacional Monetario emitió una resolución primera en su estilo que obligaba a entidades financieras reguladas por el banco central a gestar políticas internas propias de ciberseguridad. Es así que, a partir de este hito en el sector financiero las organizaciones se plantearon autorregularse para fortalecer la ciberseguridad.

Como se observa de manera parecida que en el caso japonés la regulación brasileña también requiere que el sector financiero desarrolle lineamientos de ciberseguridad, o también llamadas estrategias de “autonomía” y “autogobierno” con la finalidad de responder ante incidentes, y cumplir con estándares a la hora de ofertar al público la contratación de servicios financieros por parte de dicha industria.

2. Conclusiones

- Se ha resaltado la experiencia comparada de siete países y la Unión Europea en torno a la prevención del cibercrimen. De acuerdo con la investigación académica de Kshetri y Kshetri (2016) y el reporte de ciberseguridad elaborado por el BID y la OEA (2020), el criterio para elegir a dichos países se basó en su influyente protagonismo internacional en el ámbito de políticas de ciberseguridad y/o ciberdefensa. Como se ha visto, hay países que han desplegado continuos esfuerzos por adoptar normativa adecuada contra el cibercrimen.

- Con respecto a EE. UU. y Brasil, las primeras regulaciones en torno a ciberseguridad se dieron en las instituciones financieras debido a los frecuentes riesgos asociados a ciberataques puros dirigidos a las arquitecturas del *software* financiero. Así, tal como indica Tropina & Callanan (2015), los marcos de ciberseguridad específicos al sector económico/financiero fueron uno de los primeros enfoques regulatorios en el mundo. A partir de las iniciativas de los países revisados, este enfoque calzaría la definición de enfoque co-regulatorio (*top-down*) propuesta por los autores mencionados, en la medida que existe un fuerte componente de intervención y observancia estatal.

- En relación con las finalidades que buscarían las estrategias de ciberseguridad entre países, se dijo que la ciber-estrategia estadounidense está impulsada por visiones y prioridades distintas en comparación con la de la Unión Europea. Es así que la ciber-estrategia norteamericana se enfoca más en la lucha contra las ciber-amenazas y en el despliegue de ciber-operaciones ofensivas mediante ciberataques preventivos, mientras que la estrategia de la Unión Europea ahonda en el fortalecimiento de un marco basado en principios que proporciona un modelo para las buenas prácticas (Brandon, 2014).

- Se resaltó que hay países que realizan sustanciales mejoras de manera gradual a lo largo de los años para avanzar el desarrollo y capacidades de sus ecosistemas de ciberseguridad. Un ejemplo de estos casos es el de Israel, país que durante de diez años aproximadamente elaboró una sólida y coherente estrategia nacional de ciberseguridad adecuada a su marco político integral, además de convertirse en un centro global de excelencia para la investigación y la ciberseguridad (Press, 2017; Leitersdorf & Schreiber, 2019).

- Se indicó que Japón es un ejemplo de agente estatal con políticas regulatorias sobre ciberseguridad que minimizan la regulación directa y favorecen intervenciones del sector privado para generar estándares de ciberseguridad en sus respectivas industrias. Este enfoque se ha realizado a través de diversas estrategias nacionales que promueven políticas importantes en lugar de un marco regulatorio más restrictivo (Shackelford, Russell & Haut, 2016). Como se observó, las estrategias japonesas de ciberseguridad destacan el énfasis en la participación voluntaria del sector privado de abajo hacia arriba -*bottom up approach*-, conocida como estrategias de "autonomía" y "autogobierno" (Shackelford, Russell & Haut, 2016).

- El enfoque japonés es un ejemplo adecuado con lo que Tropina & Callanan (2015) definen como auto-regulación, en la medida que es principalmente iniciado por actores privados y establecido independientemente de la adopción de órdenes legales, lo que no significa que el estado se mantenga alejado del esfuerzo necesario para imponer la auto-regulación. Es así como muchas formas de auto-regulación incluyen al estado como iniciador o participante. Como sostiene Shackelford, Russell & Haut (2016), la estrategia japonesa proporciona protecciones básicas de privacidad y exige que los controladores de datos tomen las medidas necesarias y adecuadas para la prevención de fugas, pérdidas o daños; y para otros controles de seguridad de los datos personales.

- Asimismo, se demostró que dos de los denominados países BRICS, como China y Rusia, no conceden necesariamente las mismas libertades digitales en las esferas de libertad de expresión, acceso a la información, privacidad y protección de datos, a sus ciudadanos en comparación con sus pares occidentales. De ahí se sigue qué si bien todos los países examinados cuentan con claras y definidas normativas de ciberseguridad implementadas y en funcionamiento (Marco legal y regulatorio), no quiere decir que todos respeten los derechos fundamentales de sus ciudadanos por igual.

- Es así que China tras su intención de construir fronteras para el ciberespacio dentro de su arquitectura de internet, es decir, el "Gran Cortafuegos" -*The Great Firewall*- ha facilitado eficazmente el filtrado y el bloqueo de contenido extranjero en línea (Huang & Mačák, 2017; Yuen, 2015; Iasiello, 2017).

- En esta línea, Rusia mediante la implementación de la llamada ley "Telón de acero en línea" buscaría un funcionamiento sostenible del internet ruso, en caso el país fuera desconectado del resto de la red global (Rodgers, 2019). Además de obligar a los proveedores de servicios de Internet a instalar equipos especiales que puedan rastrear, filtrar y desviar el tráfico de Internet. Permitiendo de esta manera al regulador de telecomunicaciones ruso, Roskomnadzor, bloquear de forma independiente y extrajudicial el acceso a contenido que el gobierno considera una amenaza (Human Rights Watch Org, 2020).

- Luego de analizar la experiencia comparada de estos ocho países en torno a la prevención y persecución de la actividad cibercriminal, se recomienda contar con

un marco legal adecuado para que los Estados apliquen normativas pertinentes que posibiliten combatir de manera eficiente la cibercriminalidad. En este sentido, no es posible combatir la ciberdelincuencia en igualdad de armas con otros agentes estatales, si existe un grupo de ellos que no cuenta con el conocimiento empírico y la experiencia acumulada en dichos entornos regulatorios y/o normativos.

- Como se ha visto en el análisis de los países bajo estudio, en todas las regiones se presentan contextos de ciberseguridad distintos, donde las ventajas de algunos países no las comparte el resto de estados. Estas diferencias obedecen a razones de diversa índole, como de naturaleza presupuestal, de política criminal, de políticas de prevención, entre otros factores.

- Por su parte, la agencia especializada de las Naciones Unidas - ITU - Unión Internacional de Telecomunicaciones - sostiene que las estrategias contra el cibercrimen desarrolladas en países industrializados deben introducirse en los países en desarrollo de manera progresiva, con la finalidad de ofrecer ventajas de reducción de costos y tiempo, para implementarlas y desarrollarlas de manera adecuada y exitosa (Gercke, 2012).

- Si bien los países desarrollados como aquellos en vía de desarrollo enfrentan desafíos similares en torno a la -ciberdelincuencia-, la adopción de soluciones óptimas depende de la disponibilidad de recursos y capacidades técnicas de cada país, por esta razón los estados industrializados son capaces de promover estrategias de ciberseguridad de formas distintas, así como flexibles (Gercke, 2012).

- Existen factores que los países en vías de desarrollo deben considerar antes de adoptar estrategias internacionales contra el ciberdelito. Por ejemplo, algunos de estos pueden relacionarse con la compatibilidad de los respectivos sistemas legales, en aras de viabilizar el adecuado funcionamiento de estos foráneos modelos de respuesta con el desarrollo de las capacidades locales.

- Otros factores a considerar pueden ser el estado de las iniciativas de apoyo, la educación de la sociedad, el alcance de las medidas de autoprotección vigentes, así como el alcance colaborativo del sector privado, a través de asociaciones público-privadas (Gercke, 2012).

- De acuerdo con la ITU a diferencia de una estrategia de ciberdelincuencia general que puede dirigirse a varios ámbitos de incidencia y a agencias y actores responsables, el rol que debe cumplir la política cibercriminal es definir de manera clara y eficiente la respuesta gubernamental frente a la ciberdelincuencia.

- Por esta razón se recomienda que la respuesta estatal no se limite de manera exclusiva a engendrar volumétricos paquetes legislativos, pudiendo usar otras herramientas a su disposición. Como pueden ser los distintos enfoques de prevención del delito, aún si es necesario el desarrollo legislativo correspondiente, siempre se puede escoger otras vías además del derecho penal, como por ejemplo priorizar la elaboración de programas de corte preventivo del delito (Gercke, 2012).

- Desarrollar una política cibercriminal que sea concreta, pero a la vez sinérgica es fundamental, porque de esta manera se refuerza la capacidad de integrar los distintos frentes de la actividad estatal mediante esfuerzos conjuntos que aceleren respuestas idóneas al problema ciber delincuencial. En esta línea la ITU ya ha establecido que la promulgación excesiva de leyes no puede convertirse en el único medio de prevención cibercriminal disponible, dado que este proceder no está a la altura de cumplir dicha pretensión preventiva, sino que el camino ideal es asegurar que las medidas, programas, y estrategias desplegadas sean interdependientes entre sí, para que no causen fricción o conflictos entre sí, mientras coadyuvan y aceleran conjuntamente con la obtención del objetivo trazado.

- De los países bajo estudio, ha quedado evidenciado que como punto de inicio contar con legislación adecuada sobre ciberseguridad es un estadio necesario, y no excluye que otras medidas sinérgicas de carácter preventivo puedan trabajar conjuntamente de cara a hacer frente al fenómeno cibercriminal.

- Como se resaltó en el capítulo precedente, si bien el gobierno tiene un papel fundamental que desempeñar en el liderazgo de la seguridad en el ciberespacio, ya sea a través de la implementación de mecanismos tradicionales como la aplicación de la ley o mediante enfoques regulatorios menos convencionales. Se recomienda no descuidar la importancia de consolidar una sinergia con el sector

privado, ya que como señala Sales (2018) el sector privado está altamente capacitado para generar la información de la que depende la ciberdefensa.

- De acuerdo con Gercke (2012) es importante destacar que, dentro de los diferentes enfoques para armonizar la legislación sobre ciberdelincuencia, se ha dado muy poca prioridad a no solo integrar la legislación en el marco legal nacional, sino también a incluirla dentro de una política criminal existente, o desarrollar dicha política por primera vez. Como consecuencia, algunos países que simplemente introdujeron una legislación sobre el ciberdelito sin haber desarrollado una estrategia contra el ciberdelito, así como políticas a nivel gubernamental, enfrentaron graves dificultades en alcanzar los objetivos trazados. “Estos conflictos se debieron principalmente a la falta de medidas de prevención del delito, así como a la superposición de diferentes medidas” (Gercke, 2012, p. 111).

- En esta línea el tratamiento del fenómeno de la cibercriminalidad para el BID y la OEA (2020) requiere de “una política de ciberseguridad integral y sostenible, apoyada por la agenda política del país, con asignación de recursos financieros y capital humano calificado para llevarla a cabo” (p. 18).

En el siguiente capítulo se analizará la política criminal peruana frente a la cibercriminalidad pura, con la finalidad de identificar la existencia de una política cibercriminal debidamente integrada con estrategias de mitigación y prevención del ciberdelito.

CAPÍTULO 4

Política criminal y cibercriminalidad pura: el caso peruano

1. Prevalencia de la cibercriminalidad pura de acuerdo con los datos del Ministerio Público

La siguiente información revela la incidencia de denuncias en los últimos dos años con relación a los delitos informáticos de acuerdo con el boletín estadístico de marzo del 2019 elaborado por el Ministerio Público Fiscalía de la Nación; MPFN en adelante. En el 2019 se registró un total de 1,536 casos de delitos informáticos, cifra mayor en un -99.74%- a los delitos registrados en el mismo período del año 2018 que fue de 769 delitos. El delito informático con mayor incidencia fue *contra el patrimonio* con un porcentaje de -36.07%-[1] (Ministerio Público, 2019, p. 52).

A partir de la información provista es difícil concluir que la suma de los porcentajes de las categorías *contra el patrimonio* y delito *sub genérico* equivalente al -89.71%- estarían asociados necesariamente a supuestos de cibercriminalidad pura. Cabe la posibilidad que no lo estén, de igual modo, es posible que un porcentaje de delitos de cibercriminalidad pura se los trate como pertenecientes a otras modalidades, como ciberataques replica o de contenido.

Las estadísticas sobre delitos *contra datos y sistemas informáticos*, que para fines de este trabajo son sinónimo de cibercriminalidad pura, revela un incremento pronunciado cuando se compara el mes de marzo del 2018 con apenas 20 delitos con el mes de marzo del 2019 con 62 delitos.

Es así que, salvo los delitos *contra datos y sistemas informáticos* -4.04%- que pertenecen a la cibercriminalidad pura, los delitos informáticos *contra el patrimonio* -36.07%- y los delitos *sub-genéricos* -53.64%- no detallan bajo que modalidad se realizaron, lo cual podría encubrir el número real de delitos en la modalidad pura que no fueron calificados como tales, dando como resultado una cifra de negra de delitos en la modalidad pura aun no registrados en el conteo total (Ministerio Público, 2019, p. 52).

[1] Es relevante señalar que, respecto de los delitos informáticos contra el patrimonio registrados en fiscalías provinciales penales y mixtas a nivel nacional, no se especifica que modalidades se emplearon para la comisión de estos. De igual manera aquellos denominados sin especificar delito sub genérico -53.64%- tampoco lo hacen. Esto representa un problema en términos de posibilitar el acopio y posterior análisis de información crítica sobre las modalidades empleadas que viabilizaron dichos delitos.

Finalmente, sobre aquellos delitos informáticos que no suscita duda la disociación con aquellos de vertiente pura, se muestran los delitos informáticos *contra la fe pública* -3.84%-, *contra la indemnidad y libertad sexual* -1.30%-, y aquellos *contra la intimidad y el secreto de las comunicaciones* -0.78%- (Ministerio Público, 2019, p. 52).

2. Política criminal peruana frente a la cibercriminalidad pura

Como se estableció en el segundo capítulo, se entiende por política criminal toda acción estatal que se encuentra enmarcada en el modelo de Estado Constitucional de Derecho, y es conducente a resolver el problema de la criminalidad a través de su prevención.

A continuación, con fines de situarse en la política criminal peruana, se presentará las fases temporales de dicha política resumiéndola en una tabla según el año correspondiente bajo los siguientes elementos clasificadores: la norma en vigencia, la fecha de publicación, las medidas político-criminales incluidas, y su especificidad en relación a la cibercriminalidad pura.

Tabla 24
Política criminal frente a la cibercriminalidad en la década del 90

Norma	Fecha de publicación	Medidas político-criminales incluidas	¿Es específica para la cibercriminalidad pura?
Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática (INEI)	30 de abril 1990	Se crea una institución; el INEI. Normativa regulatoria.	No

Fuente: Sistema Peruano de Información Jurídica – SPIJ, elaboración propia.

Tabla 25
Política criminal frente a la cibercriminalidad en la década del 2000

Norma	Fecha de publicación	Medidas político-criminales incluidas	¿Es específica para la cibercriminalidad pura?
Ley 27309 - que incorpora los delitos informáticos al Código Penal	17 de julio 2000	Enfoque de prevención secundaria, se crea penas; para combatir supuestos de accesos ilícitos, intrusismo informático y/o *hacking;* artículos 207-A, 207-B, 207-C.	Si
Resolución Ministerial N° 181-2003-PCM	4 de junio 2003	Se implementa una medida de corte regulatorio; la Comisión Multisectorial para el Desarrollo de la Sociedad de la Información – CODESI.	No

Resolución Ministerial N° 235-2004-PCM	agosto 2004	Medida de corte regulatorio; se dispone la publicación de informes relacionados al desarrollo de la sociedad de la información en el Perú.	No
Resolución Ministerial N° 224-2004-PCM	Julio 2004	Medida de corte regulatorio; se aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información. 1ª Edición.	No
Resolución Ministerial N° 148-2005-PCM	19 de julio 2005	Medida de corte regulatorio; se dispone la publicación del Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana en el portal de la Presidencia del Consejo de Ministros.	No
Resolución Ministerial N° 318-2005-PCM	Agosto 2005	Medida de corte regulatorio; se constituyó La Comisión Multisectorial para el seguimiento y evaluación del "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana.	No
Decreto Supremo Nº 031-2006-PCM	21 de junio 2006	Medida de corte regulatorio; se aprueba el "Plan de Desarrollo de la Sociedad de la Información-La Agenda Digital Peruana".	No
Resolución Ministerial N° 246-2007-PCM	25 de agosto 2007	Medida de corte regulatorio; se aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. 2a Edición.	No
Decreto Supremo Nº 022-2017-PCM	27 de febrero 2007	Medida de corte regulatorio; se designa como ente rector del Sistema Nacional de Informática a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), encargada de implementar la Política Nacional de Gobierno Electrónico e Informática (Hoy en día SEGDI).	No
Decreto Supremo Nº 048-2008-PCM	17 de julio 2008	Medida de corte regulatorio; se aprueba la reestructuración de la Comisión Multisectorial para el Seguimiento y Evaluación del "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana".	No
Resolución Ministerial N° 360-2009-PCM	22 de agosto 2009	Medida de corte regulatorio; se crea el Grupo de Trabajo denominado Coordinador de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública del Perú (Pe-CERT), para dotar de un servicio de respuesta a incidentes de seguridad de la información que puedan manifestarse en las redes de las computadoras de la Administración Pública.	Si

Fuente: Sistema Peruano de Información Jurídica – SPIJ, elaboración propia.

Tabla 26
Política criminal frente a la cibercriminalidad en la década del 2010

Norma	Fecha de publicación	Medidas político-criminales incluidas	¿Es específica para la cibercriminalidad pura?
Decreto Supremo N° 066-2011-PCM	27 de julio 2011	Medida de corte regulatorio; se aprueba el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0" (AD 2.0), derogando el Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana del 2006 (ADP).	No
Ley N° 29733 - Ley de Protección de Datos Personales	3 de julio 2011	Medida de corte regulatorio; se garantiza el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú	No
Ley N.º 29904 - Ley de promoción de la Banda Ancha y construcción de la Red Dorsal Nacional de Fibra Óptica	20 de julio 2012	Medida de corte regulatorio; se impulsa el desarrollo, utilización y masificación de la Banda Ancha en todo el territorio nacional. En el artículo sexto se menciona el principio de "Neutralidad de Red" el cual refiere el deber de los proveedores de internet de respetar la neutralidad.	No
Ley Ni 30096 - Ley de Delitos Informáticos	21 de octubre 2013	Enfoque de prevención secundaria, medida de aplicación de la ley penal; esta ley introduce una serie de delitos al ordenamiento, entre los que se encuentran; el acceso ilícito, los atentados contra la integridad de datos y sistemas, delitos informáticos contra la indemnidad sexual, contra la intimidad y el secreto de las comunicaciones, contra el patrimonio (fraude informático), y contra la fe pública.	Si
Decreto Supremo Ni 003-2013-JUS - Aprueban Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales	22 de marzo 2013	Medida de corte regulatorio; se reglamenta que toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.	No
Reglamento de la Ley Nº 29904, Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica	4 de noviembre 2013	Medida de corte regulatorio; se establece los principios, reglas y disposiciones complementarias para la aplicación de la Ley N° 29904.	No
Ley N° 30036 - Ley que regula el Teletrabajo	15 de mayo 2013	Medida de corte regulatorio; se regula el teletrabajo, como una modalidad especial de prestación de servicios caracterizada por la utilización de tecnologías de la información y las telecomunicaciones (TIC), en las instituciones públicas y privadas.	No
Decreto Supremo N° 009-2015-TR que aprueba el Reglamento de la Ley N° 30036, Ley que regula el teletrabajo	11 de noviembre 2015	Medida de corte regulatorio; se reglamenta dentro del ámbito de aplicación de la Ley a aquellos trabajadores y servidores civiles que prestan servicios bajo la modalidad de teletrabajo; así como las personas naturales o jurídicas y entidades públicas que los emplean.	No
Resolución Ministerial N° 004-2016-PCM	8 de enero 2016	Medida de corte regulatorio; se aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la	No

		Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición.	
Resolución de Superintendencia N° 00027-2016	15 de setiembre 2016	Medida de corte regulatorio; se establece que el Reglamento de Gestión de Riesgo Operacional es aplicable a las entidades autorizadas por la SMV, y desarrolla una serie de nociones en ciberseguridad aplicables para el sector.	No
Resolución de Consejo Directivo Nº 165-2016-CD/OSIPTEL	15 de diciembre 2016	Medida de corte regulatorio; se reglamenta los principios rectores de la neutralidad de red.	No
Ley N° 30618 - Ley que modifica el Decreto Legislativo N° 1141, a fin de regular la seguridad digital.	27 de julio 2017	Medida de corte regulatorio; se modifica el Decreto Legislativo N° 1141, Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional- SINA y de la Dirección Nacional de Inteligencia-DINI, a fin de regular la seguridad digital.	No
Proyecto de mejoramiento y ampliación de los servicios de soporte para la provisión de los servicios a los ciudadanos y las empresas a nivel nacional - Proyecto (PE-L1222)	22 de noviembre 2017	Medida de corte regulatorio; se busca lograr un ahorro de casi 35 millones de soles al año por las mejoras en los servicios presenciales, como los MAC; en el índice de desarrollo en la provisión de servicios en línea de las Naciones Unidas; y, triplicar el número de transacciones diarias de intercambio de datos entre entidades gubernamentales de nivel central para la entrega de servicios, reduciendo la burocracia para los ciudadanos.	No
Decreto Supremo N° 106-2017-PCM - que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales (ACN)	9 de noviembre 2017	Medida de corte regulatorio; se establece que los Activos Críticos Nacionales (ACN) son aquellos recursos, infraestructuras y sistemas que son esenciales e imprescindibles para mantener y desarrollar las capacidades nacionales, en esa línea tanto la afectación, perturbación, o la destrucción de los Activos Críticos Nacionales (ACN) no permite soluciones alternativas inmediatas, generando grave perjuicio a la Nación.	No
Decreto Legislativo N° 1412 - Decreto Legislativo que aprueba la Ley de Gobierno Digital	13 de setiembre 2018	Medida de corte regulatorio; se norma las actividades de gobernanza, gestión e implementación en materia de tecnologías digitales, identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos. Es el primer hito normativo, que empieza a moldear un conjunto de políticas públicas posteriores que abordarían la ciberseguridad bajo la denominación de "seguridad digital".	No
Decreto Supremo N° 118-2018-PCM – Que declara de interés nacional el desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial.	30 de noviembre 2018	Medida de corte regulatorio; el gobierno digital busca aprovechar las oportunidades de las tecnologías digitales, la innovación en los procesos productivos, las aplicaciones digitales, la economía digital, entre otros, para lograr la transformación digital del Perú.	No
Decreto Supremo N° 050-2018-PCM - Decreto que establece la definición de	14 de mayo 2018	Medida de corte regulatorio; se establece la definición de Seguridad Digital de ámbito nacional, en el cumplimiento con la Segunda Disposición Complementaria Final de la Ley	No

Seguridad Digital de ámbito nacional		N°30618, Ley que modifica el Decreto Legislativo N°1441, de alcance obligatorio para todas las entidades de la Administración Pública.	
Resolución de Secretaría de Gobierno Digital N° 004-2018-PCM/SEGDI	22 de diciembre 2018	Medida de corte regulatorio; se aprueba las acciones prioritarias a cargo de quien ejerce el rol de "Líder de Gobierno Digital", busca fortalecer capacidades de funcionarios, mejorar sus procesos, y digitalización de servicios.	No
Resolución de Secretaría de Gobierno Digital N° 005-2018-PCM/SEGDI	22 de diciembre 2018	Medida de corte regulatorio; se aprueba los lineamientos para la formulación del Plan de Gobierno Digital, el cual incluye los ámbitos de seguridad, inclusión, y colaboración digital, entre otros.	No
Decreto Supremo N° 033-2018-PCM	23 de marzo 2018	Medida de corte regulatorio; se crea la Plataforma Digital Única del Estado Peruano, Gob.pe y establecen disposiciones adicionales para el desarrollo del Gobierno Digital.	No
Resolución Ministerial N° 119-2018-PCM - Resolución de creación del Comité de Gobierno Digital	8 de mayo 2018	Medida de corte regulatorio; se crea el Comité de Gobierno Digital, así como se establecen las funciones del mismo, su alcance, y los lineamientos de gestión y planificación en Gobierno Digital.	No
Resolución legislativa N° 30913 - que aprueba la adhesión al Convenio sobre la Ciberdelincuencia, también llamada Convención de Budapest (2001)	12 de febrero 2019	Enfoque prevención secundaria, medida de aplicación de la ley penal de alcance internacional, con la finalidad de armonizar la legislación a nivel nacional con la internacional para combatir de manera adecuada la cibercriminalidad. La adhesión a la convención de Budapest busca reconocer la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información.	Si
Resolución de Secretaría de Gobierno Digital N° 001-2019-PCM/SEGDI - Resolución que aprueba la directiva para compartir y usar *software* Público Peruano	17 de abril 2019	Medida de corte regulatorio; contribuye a optimizar el uso de recursos en las entidades de la Administración Pública, dado que podrán adecuar un software pre-existente en lugar de desarrollar un nuevo *software*, generando ahorro y contribuyendo al despliegue del gobierno digital y la transformación digital del Estado.	No
Resolución de Secretaría de Gobierno Digital N° 002-2019-PCM/SEGDI - Resolución que aprueba los Estándares de Interoperabilidad de la PIDE	17 de julio 2019	Medida de corte regulatorio; se aprueba los "Estándares de Interoperabilidad de la Plataforma de Interoperabilidad del Estado (PIDE)". La resolución es de cumplimiento obligatorio para todas las entidades de la Administración Pública.	No
Ley N°30999 - Ley de Ciberdefensa	26 de agosto 2019	Legislación que establece el marco normativo en materia de ciberdefensa del Estado, que tiene por finalidad regular las operaciones militares en y mediante el ciberespacio, además de defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales, y recursos claves para mantener las capacidades nacionales frente a amenazas,	Si

		o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.	

Fuente: Sistema Peruano de Información Jurídica – SPIJ, elaboración propia.

Tabla 27
Política criminal frente a la cibercriminalidad en la década del 2020

Norma	Fecha de publicación	Medidas político-criminales incluidas	¿Es específica para la cibercriminalidad pura?
Decreto de Urgencia N° 006-2020 - crea el Sistema Nacional de Transformación Digital	9 de enero 2020	Normativa regulatoria que crea una institución para fomentar e impulsar la transformación digital de las entidades públicas, las empresas privadas y la sociedad en su conjunto, en beneficio de los ciudadanos.	No
Decreto de Urgencia N°007-2020 - aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento	09 de enero 2020	Normativa regulatoria que crea el Centro Nacional de Seguridad Digital como una plataforma digital que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital, así como crear el Registro Nacional de Incidentes de Seguridad Digital que tiene por objetivo recibir, consolidar y mantener datos e información sobre los incidentes de seguridad digital reportados.	No
Resolución Fiscalía de la Nación 1503-2020 - Resolución que crea la Unidad Fiscal Especializada en Ciberdelincuencia con competencia nacional	12 de febrero 2021	Enfoque de prevención secundaria, normativa que posibilita la orientación técnico-jurídica en investigaciones fiscales de delitos cometidos por la ciberdelincuencia a lo largo del territorio nacional.	Si

Fuente: Sistema Peruano de Información Jurídica – SPIJ, elaboración propia.

3. Clasificación de medidas político criminales frente a la cibercriminalidad pura

Como se observa la política criminal peruana frente a la cibercriminalidad pura ha atravesado por distintas fases desde el año 1990 hasta la actualidad, el énfasis de la normativa principalmente ha recaído en ciertos aspectos regulatorios priorizando algunos ambitos por encima de otros, con la finalidad de presentar una política cibercriminal mínimamente congruente y articulada. Es así que muchas de las normas implementadas a la fecha han buscado forjar marcos regulatorios legales no existentes al momento de los hechos, por lo que la iniciativa legislativa se ha dirigido

mayoritariamente a engendrar normativa que posibilite empezar a hablar de un incipiente ecosistema digital situado en un naciente marco legal *ad hoc*.

Ejemplos de regulación del espacio digital y las TIC incluyen desde el tratamiento de datos personales, la promoción de la inclusión social a través del desarrollo y masificación de la Banda Ancha, así como planes de desarrollo de agenda y/o gobiernos digitales con la finalidad de implementar mecanismos que mejoren la seguridad digital de la información a lo largo del ámbito nacional.

Sin embargo, para los fines de este capítulo se analizará cual ha sido el despliegue político criminal exclusivamente sobre la cibercriminalidad pura y no con relación a otras modalidades como pueden ser las de réplica o contenido. Después de comparar un total de 40 medidas político criminales que buscan ya sea de manera directa o indirecta combatir y/o prevenir la cibercriminalidad implementadas desde la década de los noventa hasta la actualidad, se ha identificado un subgrupo de seis que tienen incidencia directa en la cibercriminalidad pura, siendo estas medidas las siguientes:

3.1 Medidas político criminales con enfoque de prevención secundaria

a. Ley 27309 - que incorpora los delitos informáticos al Código Penal (2000)

En la década del 2000 se incorporaron tres artículos al Código Penal relacionados con delitos informáticos mediante la Ley N° 27309. La implementación de esta Ley es de manera indubitable el primer ejercicio legislativo por penar aquellos supuestos de la modalidad pura, como es: el intrusismo informático o *hacking*. Por el tipo de medida de prevención la normativa se encuadra en la prevención secundaria del delito la cual se refleja o se ve plasmada en la política legislativa penal. Esta medida político criminal refleja la criminalización del ilícito de intrusismo informático o *hacking,* el cual integra el catálogo de delitos propios de la cibercriminalidad pura.

b. Ley N° 30096 - Ley de Delitos Informáticos (2013)

En el año 2013 se materializa un hito decisivo para combatir la cibercriminalidad pura, a través de la entrada en vigencia de la Ley de Delitos Informáticos - Ley N° 30096 que

previene y sanciona las conductas que afectan sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante el uso de tecnologías de la información o de la comunicación, para esta de manera aegurar la lucha eficaz contra la ciberdelincuencia. Este es otro ejemplo de prevención secundaria mediante la aplicación de una ley penal especial para combatir el emergente catálogo de delitos informáticos que conforman la cibercriminalidad pura, y demás vertientes.

c. Ley N°30999 - Ley de Ciberdefensa (2019)

En este año se promulgó la Ley N°30999 - Ley de Ciberdefensa con el objetivo de instaurar el marco normativo en materia de ciberdefensa del Estado, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia. La ley busca la protección de la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.

Esta iniciativa de prevención secundaria del delito busca reforzar la política criminal destinada a combatir la cibercriminalidad pura, es así que a lo largo de la norma se hace mención reiteradamente a la necesidad de combatir amenazas o ataques en y mediante el ciberespacio que afecten la seguridad nacional.

Sin embargo, a más de dos años de la entrada en vigencia de dicha ley aún no se ha publicado el reglamento correspondiente. Lo que deja a la sociedad en una situación de incertidumbre e indefensión con respecto a cómo se protegería y prevendría concretamente los supuestos de modalidad pura que atenten contra la seguridad nacional.

d. Resolución legislativa N° 30913 - que aprueba la adhesión al Convenio sobre la Ciberdelincuencia, también llamada Convención de Budapest (2019)

En el año 2019 con la aprobación de la adhesión al Convenio sobre la Ciberdelincuencia también llamada Convención de Budapest (2001), se consolida una importante medida de aplicación de la ley penal con alcance internacional, con la finalidad de armonizar la legislación doméstica con la extranjera para combatir de manera conjunta y adecuada los supuestos de modalidad pura que se susciten en el país.

Este es otro ejemplo del carácter vinculante de un instrumento jurídico internacional que se encuadra en la prevención secundaria del delito, asegurando la eficacia necesaria en la lucha contra la ciberdelincuencia. De acuerdo al informe explicativo del convenio sobre la ciberdelincuencia núm.185 del año 2001 del Consejo de Europa, este tiene como finalidad fundamental:

I) Armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada país y las disposiciones conexas en materia de delitos informáticos;

II) Establecer conforme al derecho procesal penal de cada país los poderes necesarios para la investigación y el procesamiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico,

III) Consolidar un régimen rápido y eficaz de cooperación internacional.

3.2 Medidas políticos criminales de estrategias de prevención situacional

a. Resolución Ministerial N° 360-2009-PCM (2009)

En el año 2009 mediante Resolución Ministerial N° 360-2009-PCM se crea el Grupo de Trabajo denominado Coordinador de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública del Perú (Pe-CERT), este ente sería el encargado de liderar los esfuerzos para resolver, anticipar y enfrentar los desafíos informáticos y coordinar la defensa ante los ciberataques, con el fin de proveer a la nación de una postura Segura en el Ámbito de la Seguridad Informática (pecert.gob.pe 2020).

Aquí se aprecia un importante paso en buscar la protección de los activos nacionales que podrían verse vulnerados mediante ciberataques, es así que de manera directa el despliege operativo de este grupo coordinador combatiría supuestos de la modalidad pura. Por el tipo de medida de prevención la normativa se encuadra dentro de los métodos de prevención situacional, en la medida que dota de capacidades técnicas a un grupo especializado para que lidere esfuerzos frente a la proliferación de ciberataques, y así conseguir la reducción de oportunidades, aumento del riesgo, y la

dificultad de ofender.

b. Resolución Fiscalía de la Nación 1503-2020 - Resolución mediante la cual se crea la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional (2021)

En el año 2021, se da la más significativa medida a nivel nacional para hacerle frente a la cibercriminalidad pura, se trata de la Resolución Fiscalía de la Nación N° 1503-2020, Resolución mediante la cual se crea la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional. Esta unidad especializada con competencia nacional que dependerá tanto administrativa como funcionalmente de la Fiscalía de la Nación, funcionará para una mejor coordinación nacional bajo la designación de un punto de contacto en cada distrito fiscal, quien a su vez conformará la "Red de fiscales en ciberdelincuencia a nivel nacional".

Siendo algunas de las funciones de esta Unidad Fiscal Especializada en Ciberdelincuencia las siguientes:

I) Brindar acompañamiento técnico a los fiscales en la realización de la investigación en los delitos de la Ley N°30096, Ley de delitos informáticos, y aquellos casos en los cuales la obtención de prueba digital sea determinante para la investigación.

II) Unificación de criterios en procedimientos y métodos de investigación en materia de ciberdelincuencia.

III) Coordinar con la Unidad de Cooperación Judicial Internacional y Extradiciones de la Fiscalía de la Nación, para el cumplimiento de sus funciones, así como para la atención de los requerimientos en el marco de la Red 24/7 del Convenio de Budapest.

Esta medida de enfoque de prevención secundaria es a la vez de corte situacional en tanto busca intervenir penalmente en ocurrencias de cibercriminalidad pura previniendo y/o combatiendo la comisión de dichos delitos, por intermedio del órgano constitucionalmente autónomo facultado para ejercer la acción penal que es el Ministerio Publico.

Es así que los ilícitos de la modalidad pura se verían perseguidos y denunciados penalmente por el MPFN que, al contar con un equipo técnico-jurídico especializado

para dicho fin, se estaría consiguiendo como sostiene Clarke y Cornish, y Welsh y Farrington la reducción de oportunidades, aumento del riesgo, y por ende la dificultad de ofender.

Esta iniciativa a cargo del MPFN ha sido fundamental para empezar a proyectar lo que podría ser el inicio de futuras implementaciones institucionales a mediano plazo, como sería la de contar con fiscalías especializadas en materia de ciberdelincuencia a lo largo del territorio nacional. Lo cual fortalecería la persecución del delito en la modalidad pura como en cualquiera de las demás.

4. Análisis de la Política criminal peruana frente a la cibercriminalidad pura

La política criminal peruana frente a la cibercriminalidad pura aún no se ha consolidado, sin embargo, se advierte que se ha empezado a articularse de manera gradual en las últimas tres décadas, siendo el caso que las intervenciones politico criminales en su mayoría han sido del tipo legislativo y/o regulatorio, concretamente mediante la prevención secundaria del delito, plasmando en la política legislativa penal iniciativas de prevención, identificación, y reducción de los costes asociados a la modalidad pura.

Las iniciativas político criminales han apostado por colocar la mayoría de iniciativas legislativas en el modelo de justicia penal, como si este fuera el único frente de prevención del delito completamente subdividido y desligado de otras estrategias de prevención, como son las de tipo situacional, del desarrollo y comunitaria, o de enfoques preventivos como los de corte primario o terciario. Salvo por la implementación del grupo de Emergencias en Redes Teleinformáticas de la Administración Pública del Perú (Pe-CERT), y la creación de la fiscalía especializada en ciberdelincuencia del MPFN, ambas medidas preventivas de tipo situacional, las demás medidas son de corte regulatorio y/o de enfoques de prevención secundaria en la medida que se dirigen a los demográficos que protagonizan el problema criminal.

Si bien se cuenta desde el 2005 con la DIVINDAT (División de Investigación de Delitos de Alta Tecnología) de la P.N.P, unidad policial dedicada a combatir el cibercrimen, y que ahora conjuntamente con la fiscalía de ciberdelincuencia coordinarán esfuerzos para combatir la cibercriminalidad pura, no existe a la fecha una política criminal, articulada y coherente que se aboque a combatir y prevenir los delitos informáticos en

general y específicamente la cibercriminalidad pura.

Es así que en la actualidad el Observatorio Nacional de Política Criminal, en tanto órgano encargado de producir evidencia empírica como insumo para la formulación e implementación de la política criminal, no cuenta con ninguna política criminal vigente para combatir y/o prevenir la cibercriminalidad pura, ni ninguna modalidad de cibercriminalidad en su defecto.

En esta línea el Consejo Nacional de Política Criminal – Conapoc, en tanto órgano multisectorial encargado de planificar, articular, supervisar y dar seguimiento a la política criminal del Estado, así como de analizar el fenómeno social del delito y de aprobar las medidas para combatirlo, contribuyendo a reducir los índices de delincuencia, tampoco cuenta en vigencia con una política criminal desplegada para combatir y/o prevenir la cibercriminalidad pura, ni ninguna vertiente de cibercriminalidad.

Además debe tenerse en cuenta que a la fecha si bien existe una política nacional de ciberseguridad, enfocada en su totalidad en la protección de la infraestructura, los datos e información del Estado, de acuerdo al Reporte Ciberseguridad 2020 del BID y la OEA, el Perú aún no cuenta con una estrategia nacional contra la ciberdelincuencia o una política cibercriminal que se encuentre en proceso de afinamiento y retroalimentación, como es el caso de otros países en la región como Chile (2017), Colombia (2016), Paraguay (2017), Argentina (2019), y Brasil (2018), quienes cuentan con normativa de esta naturaleza (BID & OEA, 2020).

En el actual estadio evolutivo en el que se estan forjando desarrollos legislativos y regulatorios de una política criminal que combata y prevenga la cibercriminalidad pura, debe resaltarse que la ejecución de la ley penal no se encuentra complementándose o unificándose de manera adecuada con otros enfoques de prevención del cibercrimen puro. El peligro de promulgar normativa penal de manera copiosa, como señaló Bjørgo (2016) es generar que los demás enfoques de prevención del cibercrimen perfectamente válidos y mutuamente incluyentes, se tornen en enfoques incongruentes o competitivos con respecto del uno al otro. Lo que a su vez como indicó Sorsby (2018) no coadyuvaría a fortalecer un plan integral de prevención del delito, centrado en el despliegue de una serie de barreras que de manera conjunta u holística producen el efecto deseado.

Por lo tanto, el análisis de la política criminal peruana vigente frente a la cibercriminalidad pura es admitir que no existe alguna, en este sentido resulta preocupante la ausencia

de coordinación e implementación de un enfoque holístico de estrategias y enfoques de prevención del delito, en consonancia con la ley penal, que como indican los profesores Back y LaPrade (2019) ayude a desplegar estructuras solidas de ciberseguridad capaces de mitigar eficazmente las ciber amenazas.

La inexistencia de una política cibercriminal unificadora de las distintas estrategias y enfoques de prevención del delito, pone en descubierto que los avances en combatir la ciberdelincuencia a lo largo de las tres últimas décadas de desarrollos normativos han sido un conjunto de normas desvinculadas de un fin común, y no una verdadera política criminal entendida como "un conjunto sistemático, cohesionado y consistente de decisiones de política gubernamental, basadas en análisis científico-sociales del fenómeno criminal, construidas con la participación del Estado y la sociedad" (Chincoya, 2013, p.103).

En el tercer capítulo Gercke (2012) advertía que, dentro de los diferentes enfoques y estrategias utilizados por los Estados para armonizar la legislación cibercriminal, se ha dado escasa importancia a integrar la legislación ad hoc dentro de un marco legal nacional, así como tampoco se ha considerado constituir dicho marco legal como parte fundamental de la política cibercriminal, en esta línea en algunos casos ni siquiera se ha desarrollado un anteproyecto de futura política cibercriminal. Por lo tanto, aquellos paises que introdujeron legislación cibercriminal sin previamente haber desarrollado una estrategia integral contra la ciberdelincuencia, así como políticas a nivel gubernamental afrontaron severas dificultades en alcanzar los objetivos trazados.

Gercke (2012) resaltó que el obstáculo o fracaso en la obtención de los resultados proyectados por las iniciativas legislativas, de aquellos países sin políticas cibercriminales vigentes, "se debió principalmente a la falta de medidas de prevención del delito, así como a la superposición de diferentes medidas" (p. 111).

En esta línea, se advierte que la ausencia de una política cibercriminal que aborde la modalidad pura ha impedido al Estado en calidad de iniciador, o participante forjar dinámicas participativas solidas, entre actores estatales y privados, creando los incentivos necesarios para estimular un determinado comportamiento colaborativo, en vez de esto se ha reforzado lo que García-Pablos de Molina (2001), denomina como "una prevención puramente "negativa", cuasi policial, sobre bases "disuasorias" que carece de operatividad, porque no incidiría en las causas del delito". (p. 423)

Ninguna de las seis medidas político criminales que inciden en la vertiente pura ha abordado la prevención primaria del delito, dejando las causas intactas de la ciberdelincuencia, al no atacar las raíces del problema sino solo aquellas manifestaciones de este. Si bien medidas de prevención primaria implican resolver situaciones carenciales criminógenas, lo que se traduce en prestaciones sociales y no mera disuasión, la ausencia de enfoques de prevención primaria revela que en tres décadas de desarrollos legislativos en torno a la cibercriminalidad no se ha abordado adecuadamente las causas, ni el impacto del fenómeno cibercriminal y por lo tanto su efectiva prevención.

En esta línea las iniciativas legislativas tampoco han incidido en la prevención terciaria dirigida a la población reclusa a fin de evitar la reincidencia, tampoco se conoce de programas piloto que ejecuten medidas preventivas del desarrollo dirigido a demográficos con factores de riesgo y/o prevención comunitaria, mediante intervenciones diseñadas para cambiar las condiciones e instituciones sociales. De ahí se sigue que las iniciativas legislativas no han contemplado estrategias de prevención del desarrollo, y/o comunitaria que den cabida a estas formas de intervenciones extrajurídicas.

Se resalta que tampoco existe ninguna aproximación programática a las estrategias de prevención cibercriminales empleadas en el extranjero, al menos no se cuenta con información pública que dé cuenta que se haya implementado alguna variación de las estrategias de auto regulación y co-regulación de asociaciones público-privadas propuesta por Tropina y Callanan (2015), la privatización de la ciberseguridad de Sales (2018), el monitoreo preventivo del cibercrimen de Dupont (2019), y el daño extracontractual de la habilitación negligente del ciberdelito de Rustad y Koeing (2005).

La no implementación de distintos enfoques de intervenciones extrajurídicas como los previamente detallados, refleja una oportunidad perdida, en la medida que la escasez de enfoques ya sean de distintas ciencias, métodos, y estrategias, no coadyuva al refinamiento de la eficiencia de los programas existentes, en el caso de que estos últimos si quiera existan, lo cual es debatible.

Por el contrario, lo implementado a la fecha en materia de política criminal deja en evidencia la prominencia del derecho penal a través de medidas de prevención secundaria, como si estas fueran las únicas y mejores vías para combatir la modalidad pura, o cualquier modalidad en su defecto.

Han pasado veintiún años desde que se empezó a articular las primeras iniciativas legales que hoy en día constituyen la columna vertebral de la política criminal en torno a la cibercriminalidad pura, sin embargo, a la fecha como sostiene Morachimo (2019) "no hay evidencia consistente que revele como han funcionado los marcos legales vinculados a la cibercriminalidad".

Aunado a lo anterior se infiere que en la actualidad existe una falta de cultura de transparencia en relación al acercamiento por parte del Estado hacia los ciudadanos a través de las TIC, un ejemplo de esto es que en el año 2013 la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) publico la Política Nacional de Gobierno Electrónico 2013- 2017. Documento en el cual se señalaba que uno de uno de los lineamientos estratégicos a implementar sería el acercamiento del Estado a los ciudadanos a través de las TIC, con acceso oportuno, inclusivo y participativo en aras de lograr una mejor transparencia, garantizando la interoperabilidad y el intercambio de datos espaciales a fin de mejorar los servicios públicos.

Sin embargo, en la práctica años después aun no es posible constatar el grado de transparencia alegado, en la medida que no se dispone de evidencia en el dominio público que revele la eficiencia de las iniciativas desplegadas en relación a la lucha y prevención de la cibercriminalidad pura, mucho menos se puede exigir la transparencia con respecto a los anteproyectos de diseño de alguna política cibercriminal, debido que a la fecha no se cuenta con ninguna, ni se tiene información que la elaboración de la misma se encontraría en ciernes.

Esta falta de transparencia también se puede encontrar como se advirtió anteriormente en las cifras reportadas por la P.N.P y el MPFN, al no estar debidamente desagregadas en la modalidad específica del delito, lo cual da como resultado una cifra negra de delitos en la modalidad pura aún no registrados en el conteo total de dichas estadísticas de divulgación pública.

Con respecto a la ciberseguridad, de acuerdo al Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM) desarrollado por El Centro Global de Capacidad en Seguridad Cibernética de la Universidad de Oxford, a solicitud del BID y la OEA para el reporte de ciberseguridad en América latina y el caribe (2020). Dentro del grupo de países andinos, donde se encuentra el Perú, este tiene un nivel promedio de madurez de seguridad cibernética de 2/5 (etapa formativa), lo que significa que para pasar al siguiente nivel de madurez se requiere “de una política de ciberseguridad

integral y sostenible, apoyada por la agenda política del país, con asignación de recursos financieros y capital humano calificado para llevarla a cabo". (BID & OEA, 2020, p. 18)

Por esta razón se recomienda la implementación de una estrategia nacional contra la ciberdelincuencia, o política cibercriminal con la finalidad que coadyuve la armonización de los objetivos buscados por la reciente promulgada Ley de ciberdefensa del año 2019, en aras de integrar adecuadamente las iniciativas político criminales de la legislación nacional con el tratado internacional de Budapest.

Otro asunto que no debe perderse de vista, en esta etapa formativa de madurez en las capacidades de ciberseguridad, está relacionado con la unidad de ciberdelincuencia del MPFN. Si bien es un contundente paso hacia la persecución penal de la modalidad pura, el acompañamiento y la capacitación técnica-jurídica no solo debe recaer exclusivamente en fiscales especializados, sino también en sus equipos legales, y en los jueces, y demás operarios vinculados con el derecho penal tecnológico o informático.

Por el momento no hay indicio que señale si el ejecutivo ha contemplado la capacidad de gasto que conllevará la dotación de los procesos de acompañamiento, entrenamiento y demás medidas de implementación técnico-jurídica por parte de los operarios de justicia a lo largo del territorio nacional, con la finalidad de abastecer al sistema en su totalidad con los mejores recursos para el óptimo desempeño de sus funciones.

A modo de conclusión, es necesario que los posteriores desarrollos legales consideren que la política criminal en torno a la cibercriminalidad pura no es mejor política por llenarse de leyes duras que castiguen más rápido, o a un mayor número de implicados. Sino por demostrar eficiencia en articular las prerrogativas del estado para garantizar la protección de los intereses esenciales del mismo, y de los derechos de los ciudadanos en el territorio bajo su jurisdicción.

En esta línea se recomienda que el futuro despliegue normativo nacional a través de la política criminal debe contemplar necesariamente un enfoque preventivo del delito de manera holística y pluridireccional que posibilite la implementación de estrategias de prevención situacional, del desarrollo, y comunitaria, así como de enfoque primario, y terciario, debido a que las estrategias de represión y disuasión exclusivamente desde el ámbito jurídico penal (prevención secundaria) actúa donde y cuando la conducta criminal se exterioriza y de manera tardía, más no en las causas que originan dicha conducta.

De ahí se sigue que la acción estatal mediante la política criminal si bien puede potencialmente ser de cualquier índole, es fundamental que para atender y comprender de manera adecuada los desafíos de la cibercriminalidad pura, se debe reconocer que "el derecho penal no es la única ni la mejor forma de combatir el crimen" (Jiménez, 2003, p. 127). Asimismo, en relación con la utilización equivocada de los enfoques preventivos del delito, así como de las estrategias en futuros despliegues normativos, el profesor García-Pablos de Molina (2001) señala acertadamente que, "Si bien ninguna política criminal realista puede prescindir de la pena, tampoco cabe degradar la prevención convirtiéndola en mera política penal. Más dureza, más Derecho Penal, no significa necesariamente menos crimen" (p. 373).

El reto de la eficiencia tiene que ser la prioridad principal en la reformulación estratégica y sectorial de toda nueva política nacional que combata el cibercrimen puro. "Si no se desarrolla en torno a ese objetivo bajo una verdadera voluntad estatal de acompañamiento constante, el futuro inmediato se irá configurando como un extendido espacio de mayores oportunidades y opciones para la proliferación de dicho delito"(Prado Saldarriaga, 2015 p. 27).

5. Conclusiones

- De acuerdo al boletín estadístico de marzo del 2019 elaborado por el MPFN, se registró en dicho año un total de 1,536 casos de delitos informáticos, cifra mayor en un 99.74% a los delitos registrados en el mismo período del año 2018 que fue de 769 delitos.

- En esta línea se indicó que los delitos informáticos contra el patrimonio (36.07%) y los delitos sub-genéricos (53.64%) no detallan bajo que modalidad se realizaron, lo cual podría encubrir el número real de delitos en la modalidad pura que no fueron calificados como tales, dando como resultado una cifra de negra de delitos en la modalidad pura aún no registrados en el conteo total.

- Con la finalidad de situarse en el desarrollo de la política criminal peruana, se presentó las fases temporales de dicha política resumiéndolas en tablas según

la década correspondiente bajo los criterios: norma, fecha de publicación, medidas político-criminales incluidas, y su especificidad en relación a la cibercriminalidad pura.

- Se reveló que muchas de las normas implementadas a la fecha han buscado forjar marcos regulatorios legales no existentes al momento de los hechos, razón por lo cual la voluntad legislativa ha priorizado mayoritariamente engendrar normativa que posibilite empezar a hablar de un incipiente ecosistema digital dentro de un marco legal adhoc.

- Después de comparar un total de cuarenta medidas para combatir y/o prevenir la cibercriminalidad implementadas desde la década de los noventa hasta la actualidad, se identificó un subgrupo de seis que tienen incidencia directa en la cibercriminalidad pura.

- Se realizó una clasificación de las medidas político criminales que inciden en la cibercriminalidad pura, cuatro de ellas fueron subsumidas dentro de la prevención secundaria del delito, siendo estas; a) Ley 27309 que incorporó los delitos informáticos al Código Penal (2000), b) Ley 30096 - Ley de delitos informáticos (2013), c) Ley N°30999 - Ley de Ciberdefensa (2019) y d) la Resolución legislativa N°30913 - que aprobó la adhesión a la Convención de Budapest (2019). Dos de ellas se subsumieron dentro de las estrategias de prevención situacional de delito, siendo estas: e) la Resolución Ministerial 360-2009 que creó el Pe-CERT, y f) la creación de la fiscalía especializada en ciberdelincuencia del MPFN con competencia nacional.

- Se evidenció deficiencias en las iniciativas político criminales que buscan combatir la cibercriminalidad pura, como la dependencia en demasía de la ejecución de la ley penal mediante la prevención secundaria en detrimento de complementar o unificar distintos enfoques de prevención del delito, como puede ser la prevención del desarrollo y comunitaria en la lucha contra la ciberdelincuencia.

- En esta línea se señaló la perdida de oportunidad que representa la ausencia de enfoques de intervenciones extrajurídicas para la prevención del delito como la

prevención primaria y/o terciaria, asi como la intervención estatal como iniciador o participante en cabeza de dinámicas participativas entre actores estatales y privados, creando los incentivos necesarios para estimular un determinado comportamiento colaborativo.

- Se señaló que en la actualidad no hay evidencia consistente que revele como han funcionado los marcos legales vinculados a la cibercriminalidad pura, esto se debe a una falta de transparencia manifiesta en relación a la divulgación de información pública en los canales oficiales de distribución, que revele la eficiencia de aquellas iniciativas legales aisladas, al no haber sido recogidas dentro de política criminal alguna, e implementadas para combatir y prevenir la cibercriminalidad pura.

- Se observó que, debido a la falta de transparencia señalada tampoco se dispone de información de acceso libre que dé cuenta de la implementación de alguna iniciativa programática equiparable a las estrategias de prevención cibercriminales empleadas en el extranjero, o alguna variación/aproximación de estas.

- En esta línea la política cibercriminal peruana que combata y prevenga el fenómeno de la cibercriminalidad pura no está en vigencia, porque no ha sido desarrollada como tal, de ahí se sigue que el Observatorio Nacional de Política Criminal, en tanto órgano encargado de generar evidencia empírica como insumo para la formulación e implementación de la política criminal, y el Consejo Nacional de Política Criminal – Conapoc, órgano multisectorial encargado de planificar, articular, supervisar y dar seguimiento a la política criminal del Estado, a la fecha no han desarrollado y/o elaborado un plan de política criminal dirigido para combatir y prevenir la cibercriminalidad pura, ni ninguna otra modalidad de ciberdelincuencia para dicho efecto.

- Se resaltó que si bien a la fecha existe una política nacional de ciberseguridad, que busca proteger la infraestructura, los datos e información del Estado, aún no se cuenta con una estrategia nacional contra la cibercriminalidad que se encuentre en proceso de afinamiento y retroalimentación, como es el caso de los demás países en la región. En este sentido se recomienda la implementación de

dicha estrategia con la finalidad de avanzar los objetivos trazados por la Ley de ciberdefensa, en aras de integrar adecuadamente las iniciativas político criminales del derecho doméstico con el tratado internacional de Budapest.

- Se recomienda que la futura política cibercriminal debe contemplar necesariamente un enfoque preventivo del delito entendido de manera holística, y pluridireccional que facilite la implementación de estrategias de prevención situacional, del desarrollo, y comunitario, así como de enfoques extrajurídicos de tipo primario, y terciario, debido a que la legislación penal actúa tarde en términos etiológicos y solamente cuando la conducta criminal se manifiesta, más no en las causas que originan el delito.

- A modo de conclusión se afirmó que el reto de la eficiencia tiene que ser la prioridad principal en la reformulación estratégica y sectorial de toda nueva política nacional que combata y prevenga el cibercrimen puro.

Conclusiones generales

1. El empleo del término "cibercrimen" según Miró (2011) denota la característica esencial de una nueva forma de criminalidad, con peculiaridades de carácter endógeno y exógeno muchas veces sin ninguna similitud comparable a ilicitos cometidos por la delincuencia en el mundo fáctico. Razón por la que es vital entender el fenomeno cibercrimal a partir de hipotesis cibercriminlogicas, que han sido elaboradas con la intencion de explicarlo, de este modo tambien es necesario adecuar el andamiaje juridico que penaliza dichas conductas para de esta manera prevenirlas.

2. La cibercriminalidad o ciberdelincuencia en la modalidad pura es una tipología situada dentro del fenómeno cibercriminal, siendo que esta última es la categoría criminológica que abarca a la primera, como a las demás que pueden ser las modalidades de réplica o de contenido.

3. La cibercriminalidad pura es aquella conducta delictiva que solo ocurre dentro del ciberespacio y que no es posible disociar la ejecución de la misma fuera de este. ejemplos de la modalidad pura son: *hacking* o intrusismo informático, propagación de virus e infecciones de *malware*, y ataques de denegación de servicios distribuidos y/o conexos como *DoS* y *DDoS*. La finalidad de estos delitos puede ser de índole económica o política.

4. La cibercriminalidad pura puede comprarse en la actualidad como si fuera un bien ofertado y distribuido dentro de mercados clandestinos que respaldan toda la cadena de valor de la industria del cibercrimen e impulsan la economía digital subterránea, un ejemplo de esto es el llamado modelo Crimen-como-Servicio -*CaaS*- o *Crime-as-a-Service.*

5. El cibercrimen al igual que toda manifestación criminal es multicausal, es en esta medida que la teoría criminológica permite explicar la relación causal entre aquellos factores identificados en la evidencia empírica de los estudios, y su correlación con las conductas delictivas que constituyen la cibercriminalidad.

6. Es fundamental tener en cuenta que ninguna teoría criminológica tiene la suficiencia conceptual o alcance abarcador como para explicar por si sola el fenómeno de la cibercriminalidad pura. Por esta razón, se recomienda que la cibercriminalidad desde

las teorías criminológicas contemporáneas debe entenderse de manera holística, multifactorial, integrada, y sinérgica, con la finalidad de evitar caer en interpretaciones teoréticas reduccionistas, que rechazan la importancia del conocimiento ciber criminológico considerado en su totalidad, la interdependencia de las teorías, así como las variadas interrelaciones de estas.

7. La ventaja de entender las operacionalizaciones de las teorías criminológicas de manera holística, posibilita que se pueda utilizar los componentes generales de todas y aquellos particulares de algunas para avanzar el entendimiento existente sobre las circunstancias y móviles que originan el proceder cibercriminal.

8. Dentro de las teorías del control; la teoría del autocontrol de Gottfredson y Hirschi (1984) si bien identificó una correlación entre una escasa capacidad de autocontrol por parte del infractor, y la descarga ilegal de piratería digital como música, películas, y *software*, no fue posible extrapolar la misma correlación con formas más complejas de cibercrímenes como *hacking*, en la medida que no quedó demostrado el papel que puede desempeñar el componente del autocontrol en actividades de *hacking* debido a la variedad de ataques que pueden etiquetarse como tal.

9. La teoría de los vínculos sociales de Hirschi (1969) evidenció que solo de manera parcial los componentes del vínculo social tienen un efecto sobre el *hacking* en adolescentes, siendo que un fuerte vínculo académico por parte de los jóvenes atenuaría la probabilidad de *hacking* en un 21%, y el apego a la supervisión parental reduciría la probabilidad en un 22%.

10. La teoría de la deriva digital de Goldsmith y Brewer (2015) propusó que la participación juvenil en cibercrímenes se incrementa en función de sentirse libre de las normas tradicionales mientras están en línea, resultado que indican desencadenaría la deriva digital juvenil, sin embargo una limitante de esta teoría es que a la fecha no hay estudio de investigación empírico que valide dicho marco conceptual.

11. Dentro de las teorías culturales; la teoría del aprendizaje social de Akers (1977), señala que tanto la asociación diferencial con pares desviados, así como las definiciones que incentivan la transgresión de la ley están significativamente relacionadas con un aumento de la cibercriminalidad.

12. La teoría de la desconexión moral de Bandura (1999) explicó que los *hackers*

empleaban mecanismos de desvinculación moral y/o técnicas de neutralización como medios para reducir la autocensura y/o culpa.

13. La teoría de las subculturas de Cohen (1955), exhibió que las experiencias fuera de línea y en línea se superponen e influyen en los valores y normas subculturales, siendo que la cultura *hacker* valora ciertas ordenes normativas en lugar de otras, estas órdenes serían justificaciones de conducta que buscan medir el efecto sobre las actitudes hacia el *hacking* y estructuran la identidad y el estatus dentro de la subcultura.

14. Dentro de las teorías de la oportunidad; la teoría de las actividades rutinarias de Felson y Cohen (1979) descubrierón que los *hackers* motivados buscarían el interés en la idoneidad del objetivo para comprometerse con el mismo. De esta manera, según la idoneidad del objetivo el ataque buscaría la necesidad de afectar un objetivo de alta visibilidad, con la finalidad de obtener estatus, o demostrar habilidad técnica dentro de la subcultura.

15. Sobre la teoría de prevención situacional del delito de Clarke (1997) se reveló que es un mecanismo preventivo adecuado para reducir la probabilidad y el impacto de ciber amenazas. Las técnicas de este tipo consiguen dificultar los ataques, en la medida que se aumentan los esfuerzos, y los riesgos involucrados en la comisión del delito.

16. Se recomienda que la política criminal moderna con enfoque preventivo del delito reconozca que las respuestas frente a la cibercriminalidad pueden ser potencialmente de cualquier índole, reconociendo que el empleo exhaustivo del derecho penal en tanto herramienta jurídica no debe considerarse como la más adecuada vía para combatir la ciberdelincuencia.

17. Los programas de orientación primaria resuelven los factores que contribuyen a materializar el fenómeno criminal, los de prevención secundaria actúan más tarde en la línea de tiempo de la conducta criminal; es decir no cuando ni donde, el conflicto criminal se produce o genera, sino cuando y donde se manifiesta, o cuando y donde se exterioriza, y los de prevención terciaria son aquellos que inciden en la población penada para evitar la reincidencia.

18. Para los fines de este trabajo se empleó el concepto de política criminal que refiere; aquel bajo la cual toda acción estatal se encuentra enmarcada en el modelo de Estado Constitucional de Derecho, y es conducente a resolver el problema de la criminalidad a

través de la prevención del delito.

19. Para Tonry (2011) existen tres estrategias de prevención del delito; a) la prevención situacional: se refiere a intervenciones diseñadas para prevenir la ocurrencia de delitos mediante la reducción de oportunidades, aumento del riesgo y la dificultad de ofender, b) la prevención del desarrollo: se refiere a intervenciones diseñadas para prevenir el desarrollo del potencial criminal en individuos, y está dirigido especialmente a personas con factores de riesgo, c) la prevención comunitaria: se refiere a intervenciones diseñadas para cambiar las condiciones e instituciones sociales, por ejemplo; familias, pares, normas sociales, clubes, y organizaciones que influyen en la delincuencia de las comunidades residenciales.

20. Las estrategias de prevención del delito, como la situacional, del desarrollo, y la comunitaria pueden actuar ya sea dentro como fuera del sistema penal, de igual manera los enfoques de prevención primaria, secundaria, y terciaria, por lo tanto, es recomendable que tanto las estrategias así como los enfoques se implementen de manera adecuada dentro de la política cibercriminal, con la finalidad de perseguir objetivos comunes de manera holística, confluente o integrada.

21. A partir de lo investigado se identificó cuatro propuestas de prevención utilizadas en la actualidad para combatir el fenómeno de la cibercriminalidad pura y demás vertientes. Estas son: Auto-Regulación y Co-Regulación de Asociaciones Público-Privadas de Tropina y Callanan (2015), Privatización de la Ciberseguridad de Sales (2018), Monitoreo Preventivo del Cibercrimen de Benoir Dupont (2019), y El Daño Extracontractual de la Habilitación Negligente del Ciberdelito de Rustad y Koening (2005).

22. La Auto-Regulación y Co-Regulación de asociaciones público-privadas de Tropina y Callanan (2015) supone forjar una dinámica participativa sólida entre actores estatales y privados mediante asociaciones público-privadas, siendo que la co-regulación se refiere a la participación directa del sector público en el proceso regulatorio -*Top-down*- , mientras que la auto regulación es iniciada por actores privados no jerárquicamente organizados y establecida independientemente de la adopción de órdenes legales, por ende, sigue un enfoque de abajo-arriba -*bottom-up*-.

23. La Privatización de la Ciberseguridad de Sales (2018) implica crear los incentivos adecuados para que los *hackers* vendan errores/fallas -*bugs*- en el mercado blanco -

white market- a proveedores que los parcharán, en lugar de venderlos a las agencias gubernamentales en el mercado gris -*grey market*- y a cibercriminales en el mercado negro -*black market*- que planean explotarlos.

24. El Monitoreo Preventivo del Cibercrimen de Benoir Dupont (2019) consiste en utilizar el potencial de las herramientas de monitoreo para cerrar la brecha en torno al desconocimiento de políticas, modelos, propuestas, o programas para combatir el cibercrimen alrededor del mundo. La utilización de las herramientas de monitoreo preventivo permitiría al público en general y a los formuladores de políticas públicas contar con conocimiento idóneo en tiempo real para determinar cuáles serían las iniciativas de intervención gubernamental o del sector privado más eficientes para controlar, combatir, y/o mitigar los daños causados en el ciberespacio por la actividad cibercriminal.

25. El daño extracontractual de la habilitación negligente del ciberdelito de Rustad y Koenig (2005) propone la promulgación de una ley que establezca una categoría nueva de daños extracontractuales, que tenga como finalidad responsabilizar a los proveedores de *software* por productos y servicios tecnológicos defectuosos que allanan el camino para que ciberdelincuentes exploten conocidas vulnerabilidades. Los autores proponen un deber de cuidado modificado que asegure la producción de *software* seguro y adecuado en el respectivo entorno de uso.

26. El programa de Auto-Regulación y Co-Regulación de asociaciones público-privadas de Tropina y Callanan (2015) es una estrategia de prevención situacional, aunque si el componente co-regulatorio (*top-down*) llegase a necesitar criminalizar conductas o modificar penas, entonces la iniciativa se situaría simultáneamente dentro del enfoque secundario de prevención del delito.

27. La propuesta de Privatización de la Ciberseguridad de Sales (2018) al igual que la Auto-Regulación y Co-Regulación de asociaciones público-privadas de Tropina y Callanan (2015), si bien inicialmente se alinean dentro de la estrategia de prevención situacional, en la medida que ambas propuestas empiezen a criminalizar conductas relacionadas a la venta de errores/fallas en el mercado gris y negro, en vez de hacerlo en el mercado blanco, modifiquen alguna pena en torno a las actividades conducidas en dichos mercados, o imponga penas por supuestos de incumplimiento en las dinámicas auto-regulatorias de las asociaciones público-privadas, no cabe duda que entonces se estaría aplicando de manera concurrente normativa jurídico penal propia del enfoque

secundario de prevención del delito.

28. El Monitoreo Preventivo del Cibercrimen de Benoir Dupont (2019) es una estrategia de prevención situacional, siendo que la implementación del monitoreo posibilitaría la movilización de diversas competencias, como es la sumatoria de esfuerzos de corte científico, legal, técnico, y social, al ser empleados de manera conjunta, combatirían la naturaleza multidisciplinar del fenómeno de la cibercriminalidad. Sin embargo, en la misma línea que las dos propuestas que anteceden, si la vigilancia de políticas coadyuva a plasmar en normativa penal los intereses de prevención recogidos durante los procesos de monitoreo internacional, entonces se estaría combinando una estrategia de prevención situacional del delito; el monitoreo preventivo, con un enfoque de prevención secundaria del delito; criminalización de conductas, o modificación de penas.

29. El daño extracontractual de la habilitación negligente del ciberdelito de Rustad y Koenig (2005) se concebió como un anteproyecto con miras a que se promulgue en una ley de responsabilidad civil, que recaía de manera directa en la responsabilidad de proveedores de *software,* debido al daño extracontractual causado por el comercio de productos y servicios tecnológicos defectuosos sin el deber de cuidado adecuado, lo que a su vez los autores argumentan habría facilitado la explotación de conocidas vulnerabilidades por parte de los ciberdelincuentes. La propuesta de esta normativa civil sobre responsabilidad por daños extracontractuales se subsume dentro de las estrategias de prevención situacional del delito.

30. Las propuestas para combatir la cibercriminalidad no distinguen entre las vertientes; pura, replica, y de contenido, necesariamente, sin embargo, las operacionalidades de estos programas ofrecen soluciones transversales que se adecúan a los objetivos de prevención y reducción de las vertientes cibercriminales. De ahí se sigue que los cuatro programas analizados para combatir la cibercriminalidad internacional inciden directamente en la reducción, lucha, y prevención de la cibercriminalidad pura, así como de las demás modalidades.

31. Se dijo en el primer capítulo que el concepto de ciberseguridad se refiere al conjunto de tecnologías, conceptos, políticas, procesos y prácticas utilizadas para proteger activos como por ejemplo, computadoras, infraestructura, aplicaciones, servicios, redes, sistemas de telecomunicaciones e información, y el ciber-entorno contra ataques, daños a la nación y acceso no autorizado.

32. En esa línea se mencionó que una estrategia de ciberseguridad hace alusión a los planes y acciones tomados para alcanzar cierto nivel de ventaja competitiva nacional y desempeño superior en el frente de la ciberseguridad, por esta razón se recomienda la implementación de una estrategia de ciberseguridad nacional, en la medida que el despliegue de esta implica desarrollar tecnología y capacitar fuerza laboral específica para que intervengan de manera eficiente dentro de la estrategia de ciberseguridad definida.

33. Con respecto al término ciber potencia se manifestó que esta hace referencia a una posición hegemónica ejercida por un Estado u organización política con la capacidad suficiente de usar el ciberespacio a su favor, creando capacidades tecnológicas asimétricas que producen influencia y predominio en entornos operativos disímiles, dicho de otra manera es aquella capacidad que puede permitirse producir resultados preferidos en el ciberespacio o en otros dominios.

34. En relación a la experiencia comparada de siete países y una comunidad política internacional como: Estados Unidos, China, Rusia, Israel, Corea del Sur, Japón, Brasil, y La Unión Europea. Estados quienes de acuerdo al reporte de ciberseguridad elaborado por el BID y la OEA (2020), ostentan un influyente protagonismo internacional en el ámbito de políticas de ciberseguridad y/o ciberdefensa. Se dijo que el Estado en tanto agente más idóneo en términos de credibilidad y legitimidad, es el encargado de implementar y financiar los recursos necesarios para garantizar que existan medidas adecuadas de ciberseguridad que protejan a sus ciudadanos y organizaciones de amenazas cibercriminales.

35. Sobre las finalidades que buscarían las estrategias de ciberseguridad entre Estados Unidos y la Unión Europea, se dijo que la ciber-estrategia estadounidense está impulsada por visiones y prioridades distintas que la de la Unión Europea. Es así que la ciber-estrategia norteamericana se enfoca más en la lucha contra las ciber-amenazas y en el despliegue de ciber-operaciones ofensivas mediante ciberataques preventivos, mientras que la estrategia de la Unión Europea ahonda en el fortalecimiento de un marco basado en principios que proporciona un modelo para las buenas prácticas.

36. Con respecto a países del bloque BRICS, como China y Rusia, quedó evidenciado que a través de implementaciones como el “Gran Cortafuegos” y el “Telón de acero digital” respectivamente, estos países no conceden las mismas libertades digitales en las esferas de libertad de expresión, acceso a la información, privacidad y protección de

datos, a sus ciudadanos en comparación con sus pares occidentales. En este sentido si bien todos los países examinados cuentan con claras y definidas normativas de ciberseguridad implementadas y en funcionamiento como marcos legales y regulatorios, no quiere decir que todos respeten los derechos fundamentales de sus ciudadanos por igual.

37. La experiencia japonesa demuestra que es posible que el Estado se sirva de políticas regulatorias sobre ciberseguridad que minimiza la regulación directa, y favorezca intervenciones del sector privado que generen estándares sectoriales de ciberseguridad. Este enfoque se ha realizado a través de diversas estrategias nacionales que promueven políticas importantes en lugar de un marco regulatorio más restrictivo.

38. En cuanto a Brasil se observó que las primeras regulaciones en torno a ciberseguridad se dieron en las instituciones financieras debido a los frecuentes riesgos asociados a ciberataques puros dirigidos a las arquitecturas del *software* financiero, con respecto a Corea del Sur se mencionó la oportuna implementación de una ciber-estrategia nacional desde la década del dos mil diez, como parte de una exitosa ciber-agenda de medidas para prevenir la cibercriminalidad, por su lado Israel es considerada en la actualidad una ciber potencia en la medida que se ha convertido en un centro global de excelencia para la investigación y la práctica de la ciberseguridad.

39. Luego de analizar la experiencia comparada de los Estados en torno a la prevención y persecución de la actividad cibercriminal, se concluyó que es fundamentar contar con un marco legal adecuado para que los Estados apliquen normativas pertinentes que posibiliten combatir de manera eficiente la cibercriminalidad. En este sentido, no es posible combatir la ciberdelincuencia en igualdad de armas con otros agentes estatales, si existe un grupo de ellos que no cuenta con el conocimiento empírico y la experiencia acumulada en dichos entornos regulatorios y/o normativos.

40. Se recomendó a partir de los países bajo estudio la necesidad crítica de contar con legislación adecuada sobre ciberseguridad, en tanto es un estadio necesario para combatir la ciberdelincuencia, y no excluye que otras medidas sinérgicas de carácter preventivo puedan trabajar conjuntamente de cara a hacer frente al fenómeno cibercriminal.

41. En esta línea de acuerdo con Gercke (2012) es primordial destacar que, entre las

distintas líneas programáticas para armonizar la normativa de ciberdelitos, se ha subestimado la importancia de incorporar los paquetes legislativos, medidas regulatorias, y demás herramientas de distinta naturaleza dentro del marco legal vigente como parte de una política cibercriminal de gran alcance, sinérgica, y abarcadora.

42. Para Gercke (2012) la batalla contra el cibercrimen no se gana mediante la inmediata promulgación de normativa cibercriminal dispersa, o a través de la superposición de medidas gubernamentales de agencias no interconectadas entre sí, sin haber priorizado la construcción de una ciber estrategia detallada que señale de que manera se resolverán las carencias y adversidades vigentes. Por lo tanto, la problemática de una ciber estrategia ineficiente debe su origen a la falta de planeamiento cohesionado, estratégico y sinérgico, mediante normativa y líneas programáticas diseminadas que no hablan entre sí al estar aisladas unas de otras, y por ende las capacidades y recursos para alcanzar el mismo objetivo también se encuentran dispersos. Aunado a esto la no utilización de enfoques preventivos del delito solo agrava la indefensión frente al avance de la cibercriminalidad, en tanto no se cuenta con un plan integrador de medidas y/o enfoques de por dónde empezar la prevención y de qué manera hacerlo.

43. Después de comparar un total de cuarenta medidas para combatir y/o prevenir la cibercriminalidad implementadas desde la década de los noventa hasta la actualidad, se identificó un subgrupo de seis que tienen incidencia directa en la cibercriminalidad pura.

44. Dentro de las medidas político criminales que inciden en la cibercriminalidad pura, cuatro de ellas fueron subsumidas dentro del enfoque de prevención secundaria del delito, siendo estas; I) Ley 27309 que incorporó los delitos informáticos al Código Penal (2000), II) Ley 30096 - Ley de delitos informáticos (2013), III) Ley N°30999 - Ley de Ciberdefensa (2019) y IV) la Resolución legislativa N°30913 - que aprobó la adhesión a la Convención de Budapest (2019).

45. Las dos restantes se subsumieron dentro de las estrategias de prevención situacional de delito, siendo estas: i) la Resolución Ministerial 360-2009 que creó el Pe-CERT, y ii) la creación de la fiscalía especializada en ciberdelincuencia del MPFN con competencia nacional.

46. Se señaló que en la actualidad no existe una política criminal que tenga como finalidad combatir y/o prevenir el fenómeno de la cibercriminalidad pura. Es así que el Observatorio Nacional de Política Criminal, y el Consejo Nacional de Política Criminal,

el primero órgano encargado de generar evidencia empírica como insumo para la formulación e implementación de la política criminal, y el segundo órgano multisectorial encargado de planificar, articular, supervisar y dar seguimiento a la política criminal del Estado, a la fecha no han desarrollado o elaborado un plan de política criminal dirigido para combatir y prevenir la cibercriminalidad pura, ni ninguna otra modalidad de ciberdelincuencia para dicho efecto.

47. Se resaltó la perdida de oportunidad que representa la ausencia de enfoques de intervenciones extrajurídicas para la prevención del delito como la prevención primaria y/o terciaria, así como las estrategias del desarrollo y comunitaria, además de la situacional, y modalidades de intervención estatal como iniciador o copartícipe en cabeza de dinámicas participativas entre actores estatales y privados, creando los incentivos necesarios para estimular un determinado comportamiento colaborativo.

48. Se destacó que, si bien a la fecha existe una política nacional de ciberseguridad, que busca proteger la infraestructura, los datos e información del Estado, aún no se cuenta con una estrategia nacional de seguridad cibernética que se encuentre en proceso de afinamiento y retroalimentación, como es el caso en los demás países de la región.

49. Se manifestó que en la actualidad al no contarse con una politica cibercriminal, no hay evidencia que revele como han funcionado los marcos legales vinculados a la cibercriminalidad pura, se indicó que esto se debe a una falta de transparencia manifiesta de difundir información de interés público por parte de las agencias del Estado, situación que no ayuda a valorar la efectividad de aquellos enfoques y estrategias desplegados a lo largo de tres décadas de desarrollo normativo vinculado a la cibercriminalidad.

50. Se recomendó que la futura implementación de una política cibercriminal debe contemplar necesariamente un enfoque preventivo del delito entendido de manera holística, y pluridireccional que facilite la implementación de estrategias de prevención situacional, del desarrollo, y comunitario, así como de enfoques extrajurídicos de tipo primario, y terciario, debido a que la legislación penal, en tanto prevención secundaria actúa tarde en términos etiológicos y solamente cuando la conducta criminal se manifiesta, más no en los componentes causales del ciberdelito.

Bibliografía

Abadía. M, Romero. A, Lizarazo. N. & Burgos. J. (2015) ¿Qué es la política criminal? Observatorio de Política Criminal Dirección de Política Criminal y Penitenciaria. Ministerio de Justicia y del Derecho. Bogotá, D.C., septiembre de 2015. En https://cutt.ly/igtvdJQ consulta: 8 de octubre.

Acciarri, H., Barbero, A., & Castellano, A. (1999, November). Análisis Económico de la Responsabilidad Civil: la obligación tácita de seguridad en el proyecto de reforma al Código Civil Argentino de 1998. En Anales de la XXXIV Reunión Anual de la Asociación Argentina de Economía Política.

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for cybercrime tools and stolen data: Hackers' bazaar. Rand Corporation.

Adamsky, D. (2017). The Israeli Odyssey toward Its National Cyber Security Strategy. The Washington Quarterly, 40(2), 113-127.

Abernathy, R., & McMillan, T. (2018). CISSP Cert Guide: CISSP Cert Guide, 3/e_c3. Pearson IT Certification.

Agustina, J.R. (2009). La arquitectura digital de Internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual.

Akers, R.L. (2000). Criminological Theories: Introduction, Evaluation, and Application. Third edition. Los Ángeles: Roxbury Publishing Co.

Akers, R. L. (2013). Criminological theories: Introduction and evaluation. Routledge.

Akers, Ronald L. (1998). Social Learning and Social Structure: A General Theory of Crime and Deviance. Boston, MA: Northeastern University Press.

Akers, R. L., Krohn, M. D., Lanza-Kaduce, L., & Radosevich, M. (1995). Social learning and deviant behavior: A specific test of a general theory. In Contemporary Masters in Criminology (pp. 187-214). Springer, Boston, MA.

Anandarajan, M., & Malik, S. (2018). Protecting the Internet of medical things: A situational crime-prevention approach. Cogent Medicine, 5(1), 1513349.

Anwar, S., & Loughran, T.A. (2011). Testing a bayesian learning theory of deterrence among serious juvenile offenders.

Arias Eibe, M. J. (2006). Funcionalismo penal moderado o teleológico-valorativo versus funcionalismo normativo o radical.

Arroyo, S. C. (2020). La Cibercriminología y el perfil del ciberdelincuente. Derecho y Cambio Social, (60), 470-512.

BID & OEA. (2020) Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. En: https://bit.ly/3ikfhbd consulta: 21 de agosto.

Back, Sinchul; Soor, Sadhika; and LaPrade, Jennifer (2018) "Juvenile Hackers: An Empirical Test of Self-Control Theory and Social Bonding Theory," International Journal of Cybersecurity Intelligence & Cybercrime: 1(1), 40-55.

Back, S., & LaPrade, J. (2019). The Future of Cybercrime Prevention Strategies: Human Factors and A Holistic Approach to Cyber Intelligence. International Journal of Cybersecurity Intelligence & Cybercrime, 2(2), 1-4.

Baheti, R., & Gill, H. (2011). Cyber-physical systems. The impact of control technology, 12(1), 161-166.

Bandura, A., & Walters, R. H. (1977). Social learning theory (Vol. 1). Englewood Cliffs, NJ: Prentice-hall.

Bandura, A., Barbaranelli, C., Caprara, G. V., & Pastorelli, C. (1996). Mechanisms of moral disengagement in the exercise of moral agency. Journal of personality and social psychology, 71(2), 364.

Barnes, S. (2018) There are two types of companies: Those who know they've been hacked & those who don't. En: https://bit.ly/3kZpsUg consulta: 30 de setiembre.

Bayard, E. E. (2019). The rise of cybercrime and the need for state cybersecurity regulations. Rutgers Computer and Technology Law Journal, 45(2), 69-96.

bbc.com (2019) How a ransomware attack cost one firm £45m. En: https://bbc.in/3ij6zdl consulta: 30 de setiembre.

bbc.com (2020) Amazon 'thwarts largest ever DDoS cyber-attack'. En: https://bbc.in/30nGJhS consulta: 4 de octubre.

Bederna, Z., & Szadeczky, T. (2019). Cyber espionage through Botnets. Security Journal, 1-20.

Ben-Itzhak, Y. (2008) "Organized cybercrime." ISSA Journal (October). En: https://bit.ly/3l3b51c consulta: 7 de octubre.

Bonner, E. L., III. (2014). Cyber power in 21st-century joint warfare. En: https://bit.ly/3jeciCl consulta: 12 de agosto.

Boiten, E. (2014). Nations want to be the ruler of the internet–at least within their own borders. En: https://bit.ly/3l3aJHO consulta: 12 de agosto.

Bossler, A., Burruss, G., & Holt, T. (2011). Exploring the Utility of Open-Source Data to Predict Malicious Software Creation.

Bossler, A. M., & Burruss, G. W. (2012). The general theory of crime and computer hacking: Low self-control hackers. In Cyber Crime: Concepts, Methodologies, Tools and Applications (pp. 1499-1527). IGI Global.

Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment victimization among a juvenile population. Youth & Society, 44(4), 500-523.

Bossler, A. M., & Burruss, G. W. (2010). The general theory of crime and computer hacking: Low self Control hackers? In T. J. Holt & B. Schell (Eds.), Corporate hacking and technology-driven crime: Social dynamics and implications (pp. 57-81). Hershey: IGI Global.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. Journal of Criminal Justice, 38(3), 227-236.

Bullwinkel, J. (2005). International cooperation in combating cyber-crime in Asia: Existing mechanisms and new approaches. Cyber-crime: The challenge in Asia, 269-302.

Burgess, R. L., & Akers, R. L. (1966). A differential association-reinforcement theory of criminal behavior. *Social problems*, *14*(2), 128-147.

businesswire.com (2019). The 2019 Brazilian Defense Market: Attractiveness, Competitive Landscape and Forecast to 2024. En: https://bwnews.pr/2HIdlMV consulta: 19 de agosto.

Blanco, C. (2007). Tratado de Política Criminal: Fundamentos científicos y metodológicos de la lucha contra el delito, Ed. Bosch, Barcelona.

BID (2017) Perú. Proyecto de Mejora de Servicios a Ciudadanos y Empresas (PE-L1222). En: https://bit.ly/2HGbfgt consulta: 28 de agosto.

Bjørgo, T. (2016). Preventing crime: A holistic approach. Springer.

bloomberg.com (2020) Mehrotra, K. How Hackers Bled 118 Bitcoins Out of Covid Researchers in U.S. Bloomberg. En: https://bloom.bg/3kZdpX0 consulta: 30 de setiembre.

Brandon, J. (2014). Cloud, IoT, big data require international charter on data privacy, experts claim. En: https://bit.ly/2GesyVF consulta: 07 de agosto.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cybercrime. An Analysis of the Nature of Groups engaged in Cyber Crime, International Journal of Cyber Criminology, 8(1), 1-20.

Carr, I., & Williams, K. S. (2002). Draft Cyber-Crime Convention: Criminalization and The Council of Europe (Draft) Convention on Cyber-Crime. Computer Law & Security Review, 18(2), 83-90.

Carreón, W. S. H. (2017). Revisión teórica a la génesis de la conducta criminal. Revista Electrónica de Psicología Iztacala, 20(1), 186.

Ciancaglini et al. (2015) "Below the Surface: Exploring the Deep Web." TrendMicro, Forward-Looking Threat Research Team. En: https://cutt.ly/if4qvEH consulta: 1 de octubre.

cisco.com (2020) What Is a DDoS Attack? En: https://bit.ly/2GrLaRW consulta: 4 de octubre.

cisco.com (2020) A Cisco Guide to Defending Against Distributed Denial of Service Attacks. En: https://bit.ly/3nbeAEA consulta: 5 de octubre.

Chincoya Teutli, H. (2013). ¿Política criminal, política criminológica o políticas públicas en seguridad?: reflexiones en la coyuntura de la redacción del Plan Nacional de Desarrollo 2013-2018. Alegatos-Revista Jurídica de la Universidad Autónoma Metropolitana, (83).

Chua, Y. T., & Holt, T. J. (2016). A cross-national examination of the techniques of neutralization to account for hacking behaviors. Victims & Offenders, 11(4), 534-555.

cloudflare.com (2020) What is a Denial-of-Service (DoS) Attack? En: https://bit.ly/3im3skD consulta: 1 de octubre.

cloudflare.com (2020) What is a DDoS Attack? En: https://bit.ly/3l5rd2h consulta: 2 de octubre.

cloudflare.com (2020) What was the largest DDoS attack of all time? En: https://bit.ly/30pyWAo consulta: 3 de octubre.

Cloward, R. A., & Ohlin, L. E. (1960). Delinquency and Opportunity: A theory of delinquent gangs. Free Press.

Chacon, J. (2015). Decriminalization and Its Discontents. Jotwell: The Journal of Things We Like (Lots), 2015, [380]-[382].

Choi, B. H. (2019). Crashworthy code. Wash. L. Rev., 94, 39.

Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. International Journal of Cyber Criminology, *2*(1).

Choi, K. S. (2015). Cybercriminology and digital investigation. LFB Scholarly Publishing.

Chong, J. (2013) Bad Code: The Whole Series. Lawfare. En: https://bit.ly/2EOoD1d Consulta: 17 de agosto.

Chong, J. (2013). What You Don't Know About Internet Security Will Definitely Hurt You. The New Republic. En: https://cutt.ly/DgdL6O1 consulta: 14 de octubre.

Chatin, M. (2016). Brazil: analysis of a rising soft power. Journal of Political Power, 9(3), 369-393.

Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). Cybercrime, digital forensics and jurisdiction (Vol. 593). Springer.

Choucri, N. (2012). Cyberpolitics in international relations: Context, connectivity, and content (p. 39). Cambridge, MA: MIT Press.

Cohen, A. K. (1955). Delinquent Boys: The Culture of the Gang. New York: Free Press.

Conger, K. (2016). China's New Cybersecurity Law is Bad News for Business, TechCrunch. En: https://tcrn.ch/2GISVZF consulta: 11 de agosto.

consilium.europa.eu (2020). Consejo Europeo. Consejo de la Unión Europea. Ciberseguridad en Europa: normas más estrictas y mejor protección. En: https://bit.ly/3cJTUip consulta: 8 de agosto.

Clarke, R. V. G. (Ed.). (1997). Situational crime prevention (pp. 225-256). Monsey, NY: Criminal Justice Press.

Clough, J. (2014). A world of difference: the Budapest convention of cybercrime and the challenges of harmonisation. Monash UL Rev., 40, 698.

cnn.com (2020) Australia says it has been targeted by a 'sophisticated' state-based cyber-attack En: https://cnn.it/3n9rCT1 consulta: 29 de setiembre.

Conrad, V. (2018). Digital Gold: Cybersecurity Regulations and Establishing the Free Trade of Big Data. Wm. & Mary Bus. L. Rev., 10, 295.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. Crime prevention studies, 16, 41-96.

Cox, R. W., Johnson, T. A., & Richards, G. E. (2009). Routine activity theory and Internet crime. Crimes of the Internet, 302-316.

cybersecurity.att.com (2020) Types of DDoS attacks explained. En: https://cutt.ly/Df82kB8 consulta: 6 de octubre.

De la Cuesta, José Luis y San Juan, César (2010): "La cibercriminalidad: interés y necesidad de estudio. Percepción de seguridad e inseguridad", en: de la Cuesta, José Luis (director), Derecho penal informático (Pamplona, Civitas), pp. 57-78.

Díaz, F. (2017). Mauricio Fernández, director de Ulddeco de la Fiscalía Nacional: "Se nombrarán fiscales especializados en cibercriminalidad para tener una capacidad mínima de análisis". La Tercera. En: https://bit.ly/2Sb6Fcl consulta: 8 de setiembre.

Dubrawsky, I. (2009). Eleventh Hour Security+: Exam SY0-201 Study Guide. Syngress.

Easttom, C. (2018, March). The role of weaponized malware in cyber conflict and espionage. In Proc. 13th Int. Conf. Cyber Warfare Secur.(ICCWS) (p. 191).

Eck, J. E., & Eck, E. B. (2012). Crime place and pollution: Expanding crime reduction options through a regulatory approach. Criminology & Public Policy, 11(2), 281-316.

EUCPN (2015). Cybercrime: a theoretical overview of the growing digital threat. In: EUCPN Secretariat (eds.), EUCPN Theoretical Paper Series, European Crime Prevention Network: Brussels.

EUROPOL (2018) Internet Organized Crime Threat Assessment. En: https://bit.ly/3lbgZ0t consulta: 1 de octubre.

en.itar-tass.com. (2014). Russian prosecutors urge limiting access to VKontakte over inciting extremism. En: https://bit.ly/3n5x2hP consulta: 11 de agosto.

Elías, R. (2014). Luces y sombras en la lucha contra la delincuencia informática en el Perú. En: https://bit.ly/3cNwI2H consulta: 8 de setiembre.

elperuano.pe (2019). Afianzan lucha contra ciberdelincuencia. En: https://bit.ly/2Se3n83 consulta: 9 de setiembre.

Even, S., Siman-Tov, D., & Siboni, G. (2016). (Rep.). Institute for National Security Studies.

Deibert, R., & Rohozinski, R. (2010). Control and subversion in Russian cyberspace. In J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), Access controlled: The shaping of power, rights, and rule in cyberspace. Cambridge: MIT Press.

DeLisi, M., & Vaughn, M. G. (2008). The Gottfredson-Hirschi critiques revisited: Reconciling self-control theory, criminal careers, and career criminals. International Journal of offender therapy and comparative criminology, 52(5), 520-537.

Derechos Digitales (2018). Convenio de Budapest: Aplicación en Colombia frente a derechos humanos. Fundación Karisma.

Downing, R. W. (2004). Shoring up the weakest link: What lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime. Colum. J. Transnat'l L., 43, 705.

Dupont, B. (2019). Enhancing the effectiveness of cybercrime prevention through policy monitoring. Journal of Crime and Justice, 42(5), 500-515.

Dupont, B., Côté, A. M., Boutin, J. I., & Fernandez, J. (2017). Darkode: Recruitment patterns and transactional features of "the most dangerous cybercrime forum in the world". American Behavioral Scientist, 61(11), 1219-1243.

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. White paper, Symantec Corp., Security Response, 5(6), 29.

Farmer, B. (2014). Ukraine cyber war escalates alongside violence. En: https://bit.ly/2G5aldh consulta: 13 de agosto.

Felson, M. (2013). Routine activity approach. In Environmental criminology and crime analysis (pp. 92-99). Willan.

Ferrajoli, L., & Bobbio, N. (1995). Derecho y razón: teoría del garantismo penal (p. 621). Madrid: Trotta.

ft.com (2020) Australia targeted by state-sponsored cyberattack. En: https://on.ft.com/30jvYNx consulta: 29 de setiembre.

Fiter, M. (2019) La lucha de la Policía Nacional contra el cibercrimen: "Los malos tienen más recursos". Congreso Internacional de Inteligencia Artificial. En: https://bit.ly/36pcRWi consulta: 8 de setiembre.

Frisancho, S. (2007). Desconexión moral - Albert Bandura. Revisión Teórica. http://blog.pucp.edu.pe/ En: https://cutt.ly/ogetuiE consulta: 6 de octubre.

Furnell, S. 2002. Cybercrime: Vandalizing the Information Society. Boston, MA: Addison-Wesley.

Fry, J. D. (2015). Privacy, predictability and internet surveillance in the US and China: Better the devil you know. U. Pa. J. Int'l L., 37, 419.

French, C. C. (2017). Insuring against Cyber Risk: The Evolution of an Industry. Penn St. L. Rev., 122, 607.

Froggio, G. (2007). Strain and juvenile delinquency: A critical review of Agnew's General Strain Theory. Journal of loss and trauma, *12*(4), 383-418.

García-Pablos de Molina, A. "Los retos de la moderna Criminología empírica", en Carbonell Mateu J.C./Gonzalez Cussac J.L/Orts Berenguer E. Constitución, Derechos Fundamentales y Sistema Penal, Ed. Tirant lo Blanch, Valencia, 2009.

García-Pablos de Molina, A., & Gomes, L. F. (2001). Criminología. Una Introducción a sus fundamentos teóricos para Juristas. 4ª Edición, corregida y aumentada. Edita: Tirant Lo Blanch. Valencia.

Gallagher, S. (2017). Something about Trump cybersecurity executive order seems awfully familiar, ARS TECHNICA. En https://bit.ly/30okYia consulta: 07 de agosto.

García, V. (2019) ¿Cómo está avanzando la ciberseguridad en el Perú? breve aproximación al marco normativo. Actualidad Jurídica Uría Menéndez. En: https://bit.ly/2GhFSIN consulta: 25 de agosto.

Guerrero, L. F. (2007). Seguridad pública y prevención del delito en el Estado social de derecho. Especial comentario a la trascendencia de la educación. Díkaion, 16(1).

Gerden, E. (2014). $500 million for new Russian cyber army. En: https://bit.ly/34i8NV4 consulta: 13 de agosto.

Gercke, M. (2012). Understanding cybercrime phenomena, challenges and legal response. ITU Telecommunication Development Bureau.

Gil, D. B. (2016). ¿Qué es la criminología?: Una aproximación a su ontología, función y desarrollo. Derecho y cambio social, *13*(44), 1.

Gil, J. P. (2013). Miró Linares, Fernando. El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio : Madrid: Marcial Pons, 2012. Colección: Derecho Penal y Criminología, 332 pp, ISBN 978-84-156-6418-5. Revista electrónica de ciencia penal y criminología, (15), 22.

Ghanea-Hercock, R. (2007). Survival in cyberspace. Information Security Technical Report, 12(4), 200-208.

gob.pe (2018) Nota de prensa: PCM ejecutará proyecto para simplificar y digitalizar trámites de instituciones estatales con préstamo de US$50 millones del BID. En https://bit.ly/36kgPzp consulta: 28 de agosto.

Goldberger, D., Akerman, N., Levin, J., & Ray, D. (2016). Fall 2016 Cross-Border Data Privacy Issues. Cardozo J. Int'l & Comp. L., 25, 379.

Goldsmith, A., & Brewer, R. (2015). Digital drift and the criminal interaction order. Theoretical Criminology, 19(1), 112-130.

Gómez Tabares, A. S., & Narváez Marín, M. (2019). Mecanismos de desconexión moral y su relación con la empatía y la prosocialidad en adolescentes que han tenido experiencias delictivas. Revista de Psicología (PUCP), 37(2), 603-641.

Goodman, M. (2015). Future crimes: Inside the digital underground and the battle for our connected world. Random House.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13-20.

Gorecki, J. (1974). Crime causation theories: Failures and perspectives. The British Journal of Sociology, 25(4), 461-477.

Gottfredson, M. R., & Hirschi, T. (1990). A general theory of crime. Stanford University Press.

Guarda, C. G. (2017). La política criminal aplicada (PCA): La deriva de la política criminal hacia la política pública. Nuevo Foro Penal, 13(88), 185-216.

Gulyaeva, N., & Sedykh, M. (2014). Russia enacts data localization requirement; new rules restricting online content come into effect. En: https://bit.ly/3inAy3v consulta: 14 de agosto.

Grabosky, P. (2007). Requirements of prosecution services to deal with cybercrime. Crime, law and social change, 47(4-5), 201-223.

Grabosky, P., & Walkley, S. (2007). Computer crime and white-collar crime. In International handbook of white-collar and corporate crime (pp. 358-375). Springer, Boston, MA.

Graham, S. (1998). The end of geography or the explosion of place? Conceptualizing space, place and information technology. Progress in human geography, 22(2), 165-185.

Grand, J. (1991). The theory of government failure. British journal of political science, 423-442.

fortune.com Hackett, R. (2020) What getting hacked will cost you ($3.86 million, approximately). En: https://bit.ly/2Gt2ohx consulta: 30 de setiembre.

Harcourt, B. E. (1998). Reflecting on the subject: A critique of the social influence conception of deterrence, the broken windows theory, and order-maintenance policing New York style. Michigan Law Review, 97(2), 291-389.

Huang, K., Siegel, M., & Madnick, S. (2017). Cybercrime-as-a-service: identifying control points to disrupt. MIT. Cybersecurity Interdisciplinary Systems Laboratory (CISL).

Haiminis, I. (2018). (Rep.). Institute for National Security Studies. doi:10.2307/resrep19459

Hamada, M. & Matsumoto, M. (2019) Data Protection and Cybersecurity. Chambers. Japan Law and Practice.

Harel, A. (2003). How (and Whether) to Rethink Human Rights. Int'l Legal Theory, 9, 87.

Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: an empirical analysis. Police Practice and Research, 19(6), 519-536.

Havican, R. B. (1999). La investigación criminológica y la política criminal. Cuadernos de derecho judicial, (4), 41-70.

Hei, W., & Samson, Y. U. E. N. (2015). Becoming a cyber power: China's cybersecurity upgrades and its consequences. China Perspectives, 2015(2), 53-58.

Heidenreich, S., & Westbrooks, D. (2017). Darknet Markets: A Modern Day Enigma for Law Enforcement and the Intelligence Community. American Intelligence Journal, 34(1), 38-44. doi:10.2307/26497115.

Herbert, D. T. (1982). The geography of urban crime. London: Longman.

Higgins, G. E., Fell, B. D., & Wilson, A. L. (2006). Digital piracy: Assessing the contributions of an integrated self-control theory and social learning theory using structural equation modeling. Criminal Justice Studies, 19, 3-22.

Higgins, G. E., & Makin, D. A. (2004a). Does social learning theory condition the effects of low self Control on college students' software piracy. Journal of Economic Crime Management, 2, 1-21.

Higgins, G. E., & Makin, D. A. (2004b). Self-control, deviant peers, and software piracy. Psychological Reports, 95, 921-931.

Higgins, G. E. (2005). Can low self-control help with the understanding of the software piracy problem? Deviant Behavior, 26, 1-24.

Higgins, G. E. (2006). Gender differences in software piracy: The mediating roles of self-control theory and social learning theory. Journal of Economic Crime Management, 4, 1-30.

Higgins, G. E., Fell, B. D., & Wilson, A. L. (2007). Low self-control and social learning in understanding students' intentions to pirate movies in the United States. Social Science Computer Review, 25, 339-357

Higgins, G. E., & Wilson, A. L. (2006). Low self-control, moral beliefs, and social learning theory in university students' intentions to pirate software. Security Journal, 19, 75-92.

Higgins, G. E., Wolfe, S. E., & Marcum, C. D. (2008). Digital piracy: An examination of three measurements of self-control. Deviant Behavior, 29, 440-460.

Hill, J. F. (2014). Lawfare research paper series 2(31) the growth of data localization post snowden: Analysis and recommendations for U.S. policymakers and industry leaders.

Hinduja, S., & Ingram, J. R. (2008). Self-control and ethical beliefs on the social learning of intellectual property theft. Western Criminology Review, 9, 52-72.

Himanen, P. (2015). La ética del hacker y el espíritu de la era de la información.

Hirschi, T. (1969). Causes of Delinquency. University of California Press. Berkeley, CA.

Holroyd, C. (2020). Technological innovation and building a 'super smart 'society: Japan's vision of society 5.0. Journal of Asian Public Policy, 1-14.

Holt, T. J., Brewer, R., & Goldsmith, A. (2019). Digital drift and the "sense of injustice": Counter-productive policing of youth cybercrime. Deviant Behavior, 40(9), 1144-1156.

Holt, T. J., & Kilger, M. (2008, April). Techcrafters and makecrafters: A comparison of two populations of hackers. In 2008 WOMBAT workshop on information security threats data collection and sharing (pp. 67-78). IEEE.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world. Journal of Crime and Justice, 33(2), 31-61.

Holt, T. J., Kilger, M., Chiang, L., & Yang, C. S. (2017). Exploring the correlates of individual willingness to engage in ideologically motivated cyberattacks. Deviant behavior, 38(3), 356-373.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. Deviant Behavior, 35(1), 20-40.

Holt, T. J., & Bossler, A. M. (2015). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.

Holt, T. J. (2013). Considering the social dynamics of cybercrime markets. ISP C, 77.

Holt, T. J. (2013). Examining the Forces Shaping Cybercrime Markets Online. Social Science Computer Review, 31(2), 165-177.

Holt, T. J. (2005). Hacks, cracks, and crime: an examination of the subculture and social organization of computer hackers.

Holt, T. J., Freilich, J. D., & Chermak, S. M. (2017). Exploring the Subculture of Ideologically Motivated Cyber-Attackers. Journal of Contemporary Criminal Justice, 33(3), 212-233.

Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. American Journal of Criminal Justice, 37(3), 378-395.

Holt, T. J., van Wilsem, J., van de Weijer, S., & Leukfeldt, R. (2020). Testing an integrated self-control and routine activities framework to examine malware infection victimization. Social Science Computer Review, 38(2), 187-206.

Hopkins, S. L. (2003). Cybercrime Convention: A positive beginning to a long road ahead. J. High Tech. L., 2, 101.

Huang, Z., & Mačák, K. (2017). Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches. Chinese Journal of International Law, 16(2), 271-310.

Human Rights Watch Org (2020) Russia: New Law Expands Government Control Online. En https://bit.ly/3ietia9 consulta: 15 de agosto.

Hurel, L., & Lobato, L. (2018). A Strategy for Cybersecurity Governance in Brazil (Rep.). Igarape Institute. doi:10.2307/resrep20642.1

Hurel, L (2019). Los retos de la ciberseguridad financiera en Brasil. En: https://bit.ly/3SMEq1d consulta: 5 de octubre 2022.

Hurwitz, J. (2017) Encryption Congress Mod (Apple + Calea), Harvard Journal of Law & Technology. 355, 417 n.267

Iasiello, E. (2017). China's Cyber Initiatives Counter International Pressure. Journal of Strategic Security, 10(1), 1-16.

Ingram, J. R., & Hinduja, S. (2008). Neutralizing music piracy: An empirical examination. Deviant Behavior, 29(4), 334-366.

Iclg.com (2020) Korea: Cybersecurity Laws and Regulations. En: https://bit.ly/2GhKGhg consulta: 14 de agosto.

ITU. (2008). Overview of cybersecurity, Recommendation ITU-T X.1205. The ITU Plenipotentiary Conference 2010 held in Guadalajara, Mexico, approved the definition of cybersecurity. En: https://bit.ly/30q6ZZg consulta: 6 de agosto.

ITU. (2018). Global Cybersecurity Index. En: https://bit.ly/3jmCQ4y consulta: 9 de setiembre.

Jaishankar, K. (Ed.). (2011). Cyber criminology: exploring internet crimes and criminal behavior. CRC Press.

japantimes.co.jp (2019). Japanese defense budget hits new high with focus on space and cyberspace. En: https://bit.ly/2Gewndt consulta: 15 de agosto.

Jiang, M. (2010). Authoritarian informationalism: China's approach to Internet sovereignty. SAIS Review of International Affairs, 30(2), 71-89.

Jiménez De Asua, Luis (1989). Principios de derecho penal. La ley y el delito. Argentina: Sudamericana.

Jiménez, E. B. (2003). Sobre el concepto de política criminal: Una aproximación a su significado desde la obra de Claus Roxin. Anuario de derecho penal y ciencias penales, 56(1), 113-150.

Jordan, T. and Taylor, P. 1998. A sociology of hackers. The Sociological Review 46(4): 757-780.

Jordan, T., & Taylor, P. A. (2004). Hacktivism and cyberwars: Rebels with a cause? Psychology Press.

Kallender, P., & Hughes, C. W. (2017). Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace. Journal of Strategic Studies, 40(1-2), 118-145.

Kamluk, V (2009) The botnet ecosystem. Kaspersky Publications. En: https://bit.ly/34fUdh0 consulta: 3 de octubre.

Keally, K. (2017) China's Cybersecurity Law Goes into Effect June 1, 2017–Are You Ready? NAT'L AS'N CORP. DIRECTORS. En: https://bit.ly/3kX3ilm consulta: 11 de agosto.

Kharouni, L (2012) "The Crimeware Evolution." Trend Micro Incorporated Research Paper 2012. En: https://cutt.ly/3f4envP consulta: 1 de octubre.

Khrennikov, I. (2014). Google to visa face Russia rules, boon to local data centers. En: https://bloom.bg/30n7fs1 consulta: 13 de agosto.

Klimberg, A. (2012). National cyber security framework manual. En: https://bit.ly/2Gje6eJ consulta: 06 de agosto.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. In F. D. Kramer, S. Starr, & L. K. Wentz (Eds.), Cyberpower and national security (p. 38). Washington, DC: Center for Technology and National Security, National Defense University.

Kramer, F. (2009). Cyberpower and national security. In F. D. Kramer, S. Starr, & L. K. Wentz (Eds.), Cyberpower and national security (p. 12). Washington, DC: National Defense UP.

Kshetri, N. (2012). Privacy and security aspects of social media: Institutional and technological environment. The Pacific Asia Journal of the Association for Information Systems, 3(4), 1-20.

Kshetri, N. (2015). Cybercrime and cybersecurity issues in the BRICS economies. Journal of Global Information Technology Management, 18(4), 245-249.

Kshetri, N., & Kshetri, D. N. (2016). Quest to Cyber Superiority. Springer.

Kumar, G. (2009). Cyber warfare-a global threat. International Journal of Information Technology and Knowledge Management, 2(1), 119-122.

Maimon, D., Kamerdze, A., Cukier, M., & Sobesto, B. (2013). Daily trends and origin of computer-focused crimes against a large university computer network: An application of the routine-activities and lifestyle perspective. British Journal of Criminology, 53(2), 319-343.

Malekos, Z (2022). Emerging Cyber Threats: No State Is an Island in Cyberspace. En: https://bit.ly/3CERnEB consulta: 5 de octubre 2022.

Maras, M. H. (2015). Computer forensics. Jones and Bartlett Learning.

Maras, M-H. (2017). Cyber criminology. Oxford University Press. New York, NY.

Marion, N. E., & Twede, J. (2020). Cybercrime: An Encyclopedia of Digital Crime. ABC-CLIO.

mcafee.com (2020) What Is the Difference Between Malware and a Virus? En: https://bit.ly/3n5d4E7 consulta: 30 de setiembre.

McGuire, M., & Dowling, S. (2013). Cyber-crime: A review of the evidence. Summary of key findings and implications. Home Office Research report, 75.

McIntosh, M. (1975). The organization of crime. MacMillan Publishing Company.

Matza, D. (1964). 1964 Delinquency and Drift. New York: John Wiley.

Matza, D. (1969) Becoming Deviant. New Jersey: Prentice Hall.

Medvedev S. (2020) Cybersecurity trends and issues: Russia. En: https://bit.ly/30l4Pdc consulta: 12 de agosto.

Miller, V. (2020). Understanding digital culture. SAGE Publications Limited.

Ministerio Público (2019). Boletín Estadístico. Fiscalía de la Nación - Oficina de estadística. Abril 2019. En: https://bit.ly/2G5d9XR consulta: 24 de agosto.

Moon, B., McCluskey, J. D., & McCluskey, C. P. (2010). A general theory of crime and computer crime: An empirical test. Journal of Criminal Justice, 38, 767-772.

Morachimo, M. (2019) Hiperderecho. Sentido común frente a la Convención de Budapest. En: https://bit.ly/36ikf5X consulta: 16 de mayo.

Morachimo, M. (2019) Demanda de Acción Popular a la sala constitucional de la corte superior de justicia de lima. En: https://bit.ly/34dmdSn consulta: 30 de agosto.

Morachimo M. (2019) Hiperderecho. Comentarios a la Autógrafa de Ley de Ciberseguridad aprobada por el Congreso de la República. En: https://bit.ly/3jhSAFK consulta: 28 de agosto.

mpfn.gob.pe (2017). Ministerio Público organizó con éxito Convención de Fiscales y Procuradores Generales. En: https://bit.ly/34g3ky6 consulta: 8 de setiembre.

National Security Office (2019). National Cybersecurity Strategy. En: https://bit.ly/2GmCvQA consulta: 15 de agosto.

Natapoff, A. (2015). Misdemeanor decriminalization. Vanderbilt Law Review. 68, 1055.

Nye, J. S., Jr. (2011). The future of power. New York: Public Affairs Press.

Nye, J. S. (2013). From bombs to bytes: Can our nuclear history inform our cyber future? Bulletin of the Atomic Scientists, 69(5), 8-14.

La Agenda Digital (2011) Plan de Desarrollo de la Sociedad de la Información en el Perú. En: https://bit.ly/3in4LQm consulta: 27 de agosto.

Lee, J. A. (2018). Hacking into China's Cybersecurity Law. Wake Forest L. Rev., 53, 57.

Lee, Y., & Park, J. (2015). Value creation and value capture: The case of Cybershelter for information systems security in South Korea. Journal of Information Technology Case and Application Research, 17(2), 74-92.

Leitersdorf, Y. & Schreiber, O (2019) A look back at the Israeli cyber security industry in 2018. Techcrunch. En: https://tcrn.ch/3l1AXKP consulta: 16 de agosto.

Lessig, L. (1998). The laws of cyberspace. Readings in cyberethics, 134, 136.

Leslie, K. (2008). Canadian Paediatric Society, Adolescent Health Committee, Harm reduction: An approach to reducing risky health behaviours in adolescents, Paediatrics & Child Health, Volume 13, Issue 1.

Lindsay, J. R. (2015). The impact of China on cybersecurity: Fiction and friction. International Security, 39(3), 7-47.

Loper, D. K. 2000. The criminology of computer hackers: A qualitative and quantitative analysis. (Doctoral Dissertation, Michigan State University, 2000) Dissertation Abstracts International. Volume: 61-08, Section: A, page: 3362.

Lvov, A. (2013). Russian army developing cyberattack defenses. En: https://bit.ly/36kPjC3 consulta: 13 de agosto.

Llinares, F. M. (2013). La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. Revista española de investigación criminológica, 11, 1-35.

Llinares, F. M. (2011). La oportunidad criminal en el ciberespacio. Revista Electrónica de Ciencia Penal y Criminología, 7, 1-07.

Llorens, M. P. (2017). Los desafíos del uso de la fuerza en el ciberespacio. Anuario mexicano de derecho internacional, 17, 785-816.

Manacorda, S. (Ed.). (2012). Cybercriminality: Finding a Balance Between Freedom and Security. ISPAC.

Martínez Bastida, Eduardo. Política criminológica. Prol. Alejandro Carlos Espinosa. México, Porrúa, 2007.

Mayer Lux, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. Ius et Praxis, 24(1), 159-206.

Mazerolle, L., Wickes, R., & McBroom, J. (2010). Community variations in violence: The role of social ties and collective efficacy in comparative context. Journal of Research in Crime and Delinquency, 47(1), 3-30.

Medvedev, S. (2020) Cybersecurity trends and issues: Russia En: https://bit.ly/30l4Pdc consulta: 12 de agosto.

Merrion, P. (2017) Leading Tech Firms Urge White House to Fight China's New Cyber Law, Cong. Q. Roll Call, WL 2437176.

Meyer, G. R. 1989. The social organization of the computer underground. (Master's Thesis, Northern Illinois University, 1989). En: https://bit.ly/30lDI1R consulta: 14 de mayo.

Miró Llinares, F. (2012). El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid, Marcial Pons.

Mitchell, A. D., & Hepburn, J. (2017). Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer. Yale JL & Tech., 19, 182.

Muggah, R., Garzón, J., & Suárez, M. (2018). La "Mano Dura": Los costos de la represión y los beneficios de la prevención para los jóvenes en América Latina (pp. 12-18, Rep.). Igarape Institute.

Nomokonov, V. A., & Tropina, T. L. (2012). Cybercrime as a new criminal threat. Criminology: yesterday, today, tomorrow, 24, 45-55.

Novak, M. (1993). Arquitecturas líquidas en el ciberespacio. Ciberespacio. Los Primeros Pasos, M. Benedikt (ed.), Pedro A. Gonzáles Caver (trad.). México: CONACYT/Sirius Mexicana, 207-234.

Otto, C. (2017) Los policías españoles, 'vendidos' ante el cibercrimen: "Somos pocos y nos ningunean". En: https://bit.ly/3jiOxZL consulta: 8 de setiembre.

Pacula, R. L., & Smart, R. (2017). Medical Marijuana and Marijuana Legalization. Annual review of clinical psychology, 13, 397-419.

Perry, M. J. (2003). Protecting human rights in a democracy: what role for the courts. Wake Forest L. Rev., 38, 635.

Park, J., Rowe, N., & Cisneros, M. (2016). South Korea's Options in Responding to North Korean Cyberattacks. Journal of Information Warfare, 15(4), 86-99.

Pastorino, C. (2017) Convenio de Budapest: beneficios e implicaciones para la seguridad informática. En: https://bit.ly/30opaOW consulta: 28 de agosto.

Pratt, T. C., & Cullen, F. T. (2000). The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. Criminology, 38(3), 931-964.

pecert.gob.pe (2020) ¿Que es el PECERT? En: https://bit.ly/3cPTw1F consulta: 27 de agosto.

Pocar, F. (2004). New challenges for international rules against cyber-crime. European Journal on Criminal Policy and Research, 10(1), 27-37.

nytimes.com (2020) Popper, N. Ransomware Attacks Grow, Crippling Cities and Businesses. The New York Times. En: https://nyti.ms/3n3dTx7 consulta: 30 de setiembre.

Ponemon institute (2015) The Cost of Denial-of-Services Attacks. En: https://cutt.ly/of82A4x consulta: 1 de octubre.

Posada Maya, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. Nuevo Foro Penal, 13(88), 72-112.

Prado Manrique, B. (2012) La Política Criminal contra la corrupción: Defectos y Desafíos. Comentario Jurisprudencial, IDEHPUCP.

Prado Saldarriaga, (2015). Lavado de Activos y Politica Criminal: Presente y Futuro. Problemas Actuales de Politica Criminal Anuario de Derecho Penal 2015 - 2016.

Press, G. (2019) 6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry. Forbes. En: https://bit.ly/3ikiOWM consulta: 17 de agosto.

Ramsey, C., & Wootliff, B. (2017). China's Cyber Security Law: The Impossibility of Compliance.

Ratner, S. R. (2001). Corporations and human rights: a theory of legal responsibility. The Yale Law Journal, 111(3), 443-545.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization. Criminal justice and behavior, 38(11), 1149-1169.

Reynoso Davila, R. (2004). Nociones de Criminología e Historia del Derecho Penal (3ª edición). México: Cárdenas Editor y Distribuidor.

Ripollés, J. L. D. (2011). La dimensión inclusión/exclusión social como guía de la política criminal comparada. Revista electrónica de ciencia penal y criminología, 13, 1-36.

Rodgers, J. (2019) Russia's New Internet Law: ¿Security Or Censorship? Forbes. En: https://bit.ly/30lED2j consulta: 14 de agosto.

Rogers, M. K. (2001). A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study.

Rogers, M. K., Siegfried, K., & Tidke, K. (2006). Self-reported computer criminal behavior: A psychological analysis. Lafayette: The Digital Forensic Research Conference

Romagna, M., & van den Hout, N. J. (2017, October). Hacktivism and website defacement: motivations, capabilities and potential threats. In 27th Virus Bulletin International Conference (Vol. 1, pp. 1-10).

Rosenzweig (2013) Cybersecurity and the Least Cost Avoider. Lawfare. En: https://bit.ly/3n8pHy4 consulta: 19 de agosto.

Roxin, C., Rivero, M. D. C. G., Cantizano, M. D. C. G., & Conde, F. M. (2000). La evolución de la política criminal, el derecho penal y el proceso penal. Tirant lo Blanch.

Rutherford, Andrew (Ed.) (1997), Criminal Policy Making. Aldershot: Dartmouth.

Rush, H., Smith, C., Kraemer-Mbula, E., & Tang, P. (2009). Crime online: Cybercrime and illegal innovation. Online: http://eprints. brighton.ac.uk/5800

Rustad, M. L., & Koenig, T. H. (2005). The tort of negligent enablement of cybercrime. Berkeley Technology Law Journal, 20(4), 1553-1612.

Samani, R (2013) Cybercrime: The Evolution of Traditional Crime. PRISM. En: https://bit.ly/3n9zqnX consulta: 3 de octubre.

Shackelford, S. J., Russell, S., & Haut, J. (2016). Bottoms up: comparison of voluntary cybersecurity frameworks. UC Davis Business Law Journal, 16(2), 217-260.

Shackelford, S. J., Russell, S., & Kuehn, A. (2017). Defining Cybersecurity Due Diligence Under International Law: Lessons from the Private Sector. In Ethics and Policies for Cyber Operations (pp. 115-137). Springer, Cham.

Shafa, E. K. (2014). Iran's emergence as a cyber power. En: https://bit.ly/3ijjn3g consulta: 12 de agosto.

Sales, N. A. (2018). Privatizing cybersecurity. UCLA L. Rev., 65, 620.

Sánchez Medero, G. (2012): "Cibercrimen, ciberterrorismo y ciberguerra: los nuevos desafíos del s. XXI". CENIPEC, nº 31, pp. 241-267.

Sargsyan, T. (2016). Data localization and the role of infrastructure for surveillance, privacy, and security. International Journal of Communication, 10, 17.

Suárez, J.R. (2017). We Are Cyborgs: Developing a Theoretical Model for Understanding Criminal Behaviour on the Internet.

Schia & Gjesvik (2018). The Chinese Cyber Sovereignty Concept. University of nottingham: Asia research institute. En: https://bit.ly/33jOV4A consulta: 11 de agosto.

Schmitt, M. N. (Ed.). (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press.

Schulze, E. (2019) Russia just brought in a law to try to disconnect its internet from the rest of the world. CNBC. En: https://cnb.cx/3kZqsrq consulta: 12 de agosto.

Scott, P. D. (1968). The Subculture of Violence. By Marvin E. Wolfgang and Franco Ferracuti. London: Tavistock Publications. 1967. Pp. 387. Price 63s. The British Journal of Psychiatry, 114(508), 359-359.

Serrano Maíllo, A. (2016). La teoría criminológica y sus críticos. RDUNED: revista de derecho UNED, 19, 201-220.

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. Journal of research in crime and delinquency, 34(4), 495-518.

Sims, R. L. (2002). Ethical rule breaking by employees: A test of social bonding theory. Journal of Business Ethics, 40(2), 101-109.

sputniknews.com (2017) Russia among top five countries with highest cybersecurity capabilities. En: https://bit.ly/2Sih31G consulta: 18 de agosto.

Sood, A. K., & Enbody, R. J. (2013). Crimeware-as-a-service. a survey of commoditized crimeware in the underground market. International Journal of Critical Infrastructure Protection, 6(1), 28-38.

Sorsby, A. (2018). Preventing crime: a holistic approach. International Journal of Research and Policy. Policing and Society.

Steinmetz, K. F., & Tunnell, K. D. (2013). Under the pixelated jolly roger: A study of on-line pirates. Deviant Behavior, 34(1), 53-67.

Steinmetz, K. F., & Nobles, M. R. (Eds.). (2017). Technocrime and criminological theory. Routledge.

Sterling, Bruce (1992) The Hacker Crackdown: Law and Disorder on the Electronic Frontier. New York: Bantam Books.

Summers, L. (2009). Las técnicas de prevención situacional del delito aplicadas a la delincuencia juvenil. Revista de derecho penal y criminología, (1), 395-409.

Sykes, G., Matza, D. (1957) Techniques of Neutralization: A Theory of Delinquency. American Sociological Review, Vol. 22, 664-670.

wsj.com (2020) Stupp. C. Investigators Warned Other Companies After Norsk Hydro Attack. The Wall Street Journal. En: https://on.wsj.com/2HKDuLb consulta: 30 de setiembre.

Tabansky, L. (2013). Critical infrastructure protection policy: the Israeli experience. Journal of Information Warfare, 12(3), 78-86.

theverge.com (2020) Jon Porter. Amazon says it mitigated the largest DDoS attack ever recorded. En: https://bit.ly/30H7UVp consulta: 1 de octubre.

Taylor, R. W., Caeti, T. J., Loper, D. K., Fritsch, E. J., & Liederbach, J. (2006). Digital crime and digital terrorism. Upper Saddle River, NJ: Pearson Prentice Hall, p.

Taylor, P.A. 1999. Hackers: Crime in the digital sublime. New York: Routledge.

technologyreview.com (2020). Howell O'Neill. P (2020). Una persona fallece a causa de un ciberataque por primera vez en la historia. MIT Technology Review. En: https://bit.ly/2ScyEIH consulta: 30 de setiembre.

Tejada, J. A. M. (2011). La política criminal: creencias, discursos, prácticas... saber y poder. Nuevo Foro Penal, (76), 128-149.

theguardian.com (2020) Cyber-attack Australia: sophisticated attacks from 'state-based actor', PM says En: https://bit.ly/36l7uY9 consulta: 29 de setiembre.

Thomas, D. 2002. Hacker Culture. Minneapolis, MN: University of Minnesota Press.

Thomas, T. L. (2001). Information security thinking: A comparison of U.S., Russian, and Chinese concepts. Fort Leavenworth, Ks: Foreign Military Studies Office. En: https://bit.ly/3iixPZs consulta: 12 de agosto.

Tonry, M., & Farrington, D. P. (1995). Strategic approaches to crime prevention. Crime and Justice, 19, 1-20.

Tonry, M. H. (Ed.). (2011). The Oxford handbook of crime and public policy. Oxford University Press.

cisco.com (2020) What Is the Difference: Viruses, Worms, Trojans, and Bots? En: https://rb.gy/jr9soe consulta: 30 de setiembre.

Trevino, M. (2019). Cyber Physical Systems: The Coming Singularity. PRISM, 8(3), 2-13.

Tropina, T., & Callanan, C. (2015). Self-and co-regulation in cybercrime, cybersecurity and national security (p. 25). Heidelberg: Springer.

Tropina, T. (2014, June). Fighting money laundering in the age of online banking, virtual currencies and internet gambling. In Era Forum (Vol. 15, No. 1, pp. 69-84). Springer Berlin Heidelberg.

Tropina, T. (2016). Do digital technologies facilitate illicit financial flows? World Bank, Washington, DC. © World Bank.

Tropina, T. (2013). 4. Organized Crime In Cyberspace. Heinrich-Böll-Stiftung and Regine Schönenberg (eds.) Transnational Organized Crime.

Tropina, T. (2012). The Evolving Structure of Online Criminality: How cybercrime is getting organized. In Eucrim-the European Criminal Law Associations' Forum (No. 04, pp. 158-165).

Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. International Journal of Cyber Criminology, 2(2), 382.

unodc.org (2020) Perspectives on crime causes and facilitating factors. En: https://cutt.ly/IgqFi2J consulta: 5 de octubre.

Uriostegui, E. N. M. (2010). Algunas reflexiones sobre política criminal y sus principales tendencias. Nuevo derecho, 5(6), 19-28.

Vaas, L. (2013). Infosec pros give verdict on EU's new cybersecurity strategy. En: "Nice try". https://bit.ly/30oDXch consulta: 12 de agosto.

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. Journal of Contemporary Criminal Justice, 32(2), 169-188.

Vakhitova, Z. I., Alston-Knox, C. L., Reynald, D. M., Townsley, M. K., & Webster, J. L. (2019). Lifestyles and routine activities: Do they enable different types of cyber abuse?. Computers in Human Behavior, 101, 225-237.

Wang, Q. (2016). A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe.

Wilson, J. Q., & Kelling, G. (2001). Ventanas rotas: la policía y la seguridad en los barrios. Delito y Sociedad. Revista de Ciencias Sociales, 10(15-16), 67-78.

Weimann, G. (2004): How modern terrorism uses the Internet. United States Institute of Peace, Especial Report nº 116. En: https://bit.ly/33jPH1u consulta: 29 de abril.

Weber, A. M. (2003). The council of Europe's convention on cybercrime. Berkeley technology law journal, 18(1), 425-446.

Weber, V. (2020) The Sinicization of Russia's Cyber Sovereignty Model. Council On Foreign Relations. En: https://on.cfr.org/34bjE3a consulta: 16 de agosto.

Welsh, B., Farrington, D., & Gowar, B. (2015). Benefit-Cost Analysis of Crime Prevention Programs. Crime and Justice, 44(1), 447-516. doi:10.1086/681556

Welsh, B. C., & Farrington, D. P. (2012). Crime prevention and public policy. The Oxford handbook of crime prevention, 3-19.

Welsh, B. C., & Farrington, D. P. (2010). The future of crime prevention: Developmental and situational strategies. National Institute of Justice, 1-65.

Westby, J (2019). Why The EU Is About To Seize The Global Lead On Cybersecurity. Forbes. En: https://bit.ly/2ERNh0W consulta: 13 de agosto.

Winfree Jr, L. T., Bäckström, T. V., & Mays, G. L. (1994). Social learning theory, self-reported delinquency, and youth gangs: A new twist on a general theory of crime and delinquency. Youth & Society, 26(2), 147-177.

White House, (2019). CyberSecurity Funding. Federal Budget Authority. En: https://bit.ly/30iiCBp consulta: 11 de Agosto.

Wolff, J. (2018). Trump's Reckless Cybersecurity Strategy. The New York Times. En: https://nyti.ms/36jDWdy consulta: 8 de Agosto.

Wolff, J. (2019). Cybersecurity Experts Are Leaving the Federal Government. That's a Problem. The New York Times. En: https://nyti.ms/3cMATvN consulta: 10 de agosto.

Wu, T., & Goldsmith, J. (2006). Who controls the internet? Illusions of a borderless world.

Wainwright, R., & Cilluffo, F. J. (2017). Responding to Cybercrime at Scale: Operation Avalanche--A Case Study. Center for Cyber and Homeland Security at Auburn University.

Wysocki, M. D. 2003. Cracking the hacker code: An analysis of the computer hacker subculture from multiple perspectives. (Doctoral Dissertation, Northwestern, 2003) Dissertation Abstracts International. Volume: 64-04, Section: A, page: 1125.

Wilson, A., Schulman, R., Bankston, K., & Herr, T. (2016). Bugs in The System: A Primer on the Software Vulnerability Ecosystem and its Policy Implications (pp. 15-19, Rep.). New America.

wired.com (2015) Zetter. K. The Most Controversial Hacking Cases of the Past Decade. Wired. En: https://bit.ly/2SgGTmO consulta: 29 de setiembre.

wired.com (2015) Zetter. K. Dozens Nabbed in Takedown of Cybercrime Forum Darkode. En: https://cutt.ly/7f4t75B consulta: 3 de octubre.

wired.com (2016) Zetter. K. That Insane, $81M Bangladesh Bank Heist? Here's What We Know. Wired. En: https://bit.ly/3jkjm0n consulta: 27 de setiembre.

wired.com (2018) Lily Hay Newman. GitHub Survived the Biggest DDoS Attack Ever Recorded. En: https://bit.ly/3jkBRSo consulta: 2 de octubre.

wired.com (2019) Fiveash. K. The Norsk Hydro cyberattack is about money, not war. Wired. En: https://bit.ly/3jjamsn consulta: 30 de setiembre.

Xinhua (2019). China to lead global cybersecurity market growth in next 5 years. En: https://on.china.cn/2Gds8Pm consulta: 11 de agosto.

Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. European Journal of Criminology, 2(4), 407-427.

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? The Howard Journal of Criminal Justice, 44(4), 387-399.

Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society. SAGE Publications Limited.

Young, R., & Zhang, L. (2005). Factors affecting illegal hacking behavior. AMCIS 2005 Proceedings, 457.

Yousry, F. (2018). Online Communities: An Intersection Between Computer-Mediated Communication, Subcultures and the Presentation of Self in the Global Age (Doctoral dissertation, Université d'Ottawa/University of Ottawa).

Yuen, S. (2015). Becoming a Cyber Power. China's cybersecurity upgrade and its consequences. China Perspectives, 2015(2015/2), 53-58.

Zaffaroni, E. R., Alagia, A., & Slokar, A. (2007). Derecho penal: parte general. 2a ed. Buenos Aires: Ediar.

Zekos, G. I.: "State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction". International Journal of Law and Information Technologies, 15, 1, 2007, pp. 1-37.

Zagaris, B. (2015) International Enforcement Law Reporter 31 (2015): [x]-293

Zhao, Z., Sankaran, M., Ahn, G. J., Holt, T. J., Jing, Y., & Hu, H. (2016). Mules, seals, and attacking tools: Analyzing 12 online marketplaces. IEEE Security & Privacy, 14(3), 32-43.

Zipf, H. (2010). Introducción a la política criminal. Olejnik.

Zúñiga, Laura (2001). Política criminal. Madrid: Colex.

Constituciones del Perú

- *Constitución Política del Perú (1993)*

Normas Nacionales

- Ley N° 30999, " Ley de Ciberdefensa"
- Ley N° 30096, " Ley de Delitos Informáticos"
- Ley N° 29733, " Ley de Protección de Datos Personales"
- Ley N° 27269, " Ley de Firmas y Certificados Digitales"
- Ley Nº 27309, "Ley que incorpora los delitos informáticos al Código Penal"
- Ley Nº 30618, "Decreto Legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI, a fin de regular la seguridad digital"
- La Ley N° 30036 - "Ley que regula el Teletrabajo"
- Ley N° 27291, "Ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica"
- Ley N° 29904, " Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal
- Nacional de Fibra Óptica"
- Decreto Legislativo N° 1412, "La Ley de Gobierno Digital"
- Decreto Supremo N° 065-2015-PCM, que crea la Comisión Multisectorial Permanente encargada del Seguimiento y evaluación del "Plan de desarrollo, Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0-CODESI.
- Decreto Supremo N° 081-2013-PCM, Decreto Supremo mediante el cual se aprueba la Política Nacional de Gobierno Electrónico.
- Resolución Ministerial N° 246-2007-PCM, que aprueba la Norma Técnica Peruana.
- Resolución de Superintendencia N° 00027-2016, "Reglamento de Gestión de Riesgo Operacional aplicable a las entidades autorizadas por la SMV.

Convenios

- Convenio de Budapest sobre Cibercriminalidad.