Revista Logos Ciencia & Tecnología, 15(2), 162-173 | Mayo-agosto, 2023
https://revistalogos.policia.edu.co:8443/index.php/rlct

Artículo de revisión

Revista Logos Ciencia & Tecnología
ISSN-L 2145-549X
ISSN 2422-4200 (en línea)

El control del cibercrimen. Análisis exploratorio de sentencias y medidas de supervisión

The cybercrime control. Exploratory analysis of sentences and supervision measures

Controle de crimes cibernéticos. Análise exploratória de sentenças e medidas de fiscalização

Marlon Mike Toro-Álvarez*

https://orcid.org/0000-0002-7515-8545 Southern Illinois University, Carbondale, Estados Unidos de América

- Fecha de recepción: 2023-05-05
- Fecha concepto de evaluación: 2023-06-25
- Fecha de aprobación: 2023-06-26
https://doi.org/10.22335/rlct.v15i2.1768

Para citar este artículo/To reference this article/Para citar este artigo: Toro-Álvarez, M. M. El control del cibercrimen. Análisis exploratorio de sentencias y medidas de supervisión. *Revista Logos Ciencia & Tecnología, 15*(2), 162-173. https://doi.org/10.22335/rlct.v15i2.1768

RESUMEN

El proceso de judicialización y sentencia de los individuos que han violentado la ley tiene en cuenta diferentes factores entre los que se encuentran las pautas de sentencia las cuales brindan una guía para que los jueces orienten sus decisiones durante el proceso penal. Sin embargo, la variedad de delitos y la evolución del cibercrimen requieren que esos criterios se apliquen de manera diferente, especialmente cuando nuevas tecnologías son involucradas. En el caso de los delitos cibernéticos que involucran material de abuso sexual infantil (MASI) esos criterios pueden distar de las pautas que aplican para el resto de las formas de cibercrimen. Por tal razón el presente estudio analizó 14 casos documentados en la legislación estadounidense con el fin de caracterizar las diferencias en las aplicaciones de las sentencias e indagar en las formas de supervisión para cibercriminales bajo libertad condicional. Finalmente, el presente estudio invita a reflexionar sobre los desafíos que plantean los avances tecnológicos en el control del delito y la necesidad de medidas proactivas para mejorar la respuesta de las instituciones en la contención e investigación de los delitos cibernéticos que involucran MASI.

Palabras clave: cibercrimen, criminalidad informática, explotación infantil, MASI, sentencias.

ABSTRACT

The process of prosecuting and sentencing individuals who have violated the law takes into account different factors, among which are the sentencing guidelines, which provide a guide for judges to orientate their decisions during the prosecution process. However, the variety of crimes and the evolution of cybercrime require that these criteria be applied differently, especially when new technologies are involved, in the case of cybercrimes involving child sexual abuse material (CSAM) those criteria may differ in the guidelines that apply to the other forms of cybercrime. For this reason, the present study analysed 14 documented cases in order to

* Autor de correspondencia. Correo electrónico: miketoro@bu.edu

characterise the differences in the applications of the sentences and investigate the forms of supervision for cybercriminals under probation. Finally, this study invites us to reflect on the challenges posed by technological advances in crime control and the need for proactive measures to improve the response of institutions in the containment and investigation of cybercrimes involving CSAM

Keywords: cybercrime, computer crime, child pornography, CSAM, sentence.

RESUMO

Processar e sentenciar indivíduos que tenham violado a lei levam em consideração diversos fatores, entre os quais estão as diretrizes de condenação, que fornecem um guia para os juízes tomarem suas decisões. No entanto, a variedade de crimes e a evolução dos crimes cibernéticos exigem que esses critérios sejam aplicados de forma diferente, especialmente quando estão envolvidas novas tecnologias; no caso de crimes cibernéticos com material de abuso sexual infantil, esses critérios podem diferir nas diretrizes que se aplicam às demais formas de cibercrime. Por essa razão, o presente estudo analisou 14 casos documentados, a fim de caracterizar as diferenças nas aplicações das sentenças e investigar las formas de supervisão para cibercriminosos em liberdade condicional. Por fim, este estudo nos convida a refletir sobre os desafios colocados pelos avanços tecnológicos no controle do crime e a necessidade de medidas proativas para melhorar a resposta das instituições na contenção e investigação de crimes cibernéticos que envolvam material de abuso sexual infantil.

Palavras-chave: cibercrime, crime informático, exploração infantil, CSAM, condenação.

La necesidad del control del delito cibernético

Jones y Newburn (2002) afirman que el control del delito es uno de los principales objetivos del sistema de justicia penal y de las instituciones que lo conforman. Desafortunadamente, hay delitos relacionados con el uso del ciberespacio que parecen no tener control y, por el contrario, según el *Internet Crime Complaint Center de la Oficina* de Investigaciones Federales (FBI, por su nombre en inglés; 2022), este siglo documenta un aumento de las distintas formas de ciberdelincuencia, con más de 2000 denuncias recibidas diariamente y pérdidas financieras que superan los 4200 millones de dólares al año en ataques de ciberseguridad en el continente americano, y un aumento del 1885% en los ataques dirigidos a la inutilización y los datos de las víctimas (*ransomware*; SonicWall, 2022). Este panorama motiva un mensaje de fracaso desde el papel disuasorio del castigo del delito y la forma tradicional de aplicar las sentencias (Samia, 2021).

Según Choo (2011), a diferencia de los delitos no digitales, los ciberdelitos, especialmente en redes no indexadas, son extremadamente difíciles de detectar, pueden representar un mayor nivel de victimización secundaria, afectan a un mayor número de víctimas por cada acción cibercriminal, presentan desafíos en la prevención de la reincidencia en línea y proporcionan limitaciones en el enjuiciamiento.

En cuanto a la dificultad de detección, Choi et al. (2022) afirmaron que los delitos cibernéticos requieren técnicas de investigación más elaboradas para identificarlos e individualizar a los delincuentes en línea, lo que crea una dificultad adicional para el sistema de justicia penal. Holt (2012) afirma que esta dificultad puede estar relacionada con la naturaleza de la delincuencia en línea. En estos escenarios digitales, los delincuentes pueden usar técnicas de sigilo para disfrazar su identidad y ubicación, que se derivan de las funciones disponibles en ciertos navegadores de Internet y el entorno de comunicación de la red.

Además, según Steinmetz y Yar (2019), los ciberdelincuentes pueden utilizar las capacidades del crimen organizado o individual para evadir la detección y amplificar su capacidad delictiva. Entre estas capacidades se encuentran el uso de redes privadas virtuales (VPN) o la conexión a través de servidores proxy, lo que evita el seguimiento de la actividad cibercriminal en línea.

Otra técnica que complica el seguimiento de los delincuentes digitales está relacionada con la rapidez en el cambio de los nombres de usuario y sus ubicaciones geográficas, según el explorador que utilicen Cascavilla et al., 2021). Los autores afirman que los delincuentes en línea pueden cambiar rápidamente su identidad en línea y falsificar su ubicación utilizando diferentes direcciones IP (identificadores lógicos definidos por el protocolo de Internet IP) y equipos o conexiones a redes móviles, inalámbricas o cableadas.

En cuanto al aumento de la victimización secundaria por ciberdelincuencia, Dodge y Burruss (2019) destacan cómo un ciberdelincuente puede ser arrestado y su acción ciberdelincuente aún puede estar en curso, como en el caso de una infección de software malicioso o en casos de material de abuso sexual infantil (MASI), donde las imágenes y videos siguen circulando en diferentes mercados en Internet. Esta amplificación del delito tiene impactos significativos en las víctimas, quienes pueden experimentar pérdidas financieras, daños a la reputación y afectación al bienestar emocional (Choi & Toro-Álvarez, 2017).

El estudio de Holt y Bossler (2015) destaca cómo la victimización secundaria en el ciberespacio tiene efectos persistentes y negativos en las víctimas. Esto se debe a que los datos personales robados pueden seguir circulando en repositorios ilegítimos en línea, incluso después de que se haya cometido el delito original. En casos de abuso sexual infantil, Strasburger et al. (2019) señalan que el material comprometido puede seguir distribuyéndose y compartiéndose en línea durante años, lo que causa consecuencias devastadoras para las víctimas en términos de pérdida económica, interrupción de la vida cotidiana y daño emocional y psicológico.

El ciberdelito también tiene un efecto multiplicador en términos del número de víctimas que puede afectar un solo delincuente. Por ejemplo, en ataques de denegación de servicio distribuido (DDoS), un ciberdelincuente puede convertir a más de 2000 usuarios en Internet en agentes involuntarios y atacar múltiples objetivos a través de ellos. Además, el cibercrimen puede causar un daño masivo en una escala mucho mayor que los delitos convencionales, ya que los delincuentes pueden atacar a miles de víctimas en cuestión de segundos utilizando redes de dispositivos infectados y distribuidos geográficamente (Akhgar & Brewster, 2016).

La prevención de la reincidencia en el ciberdelito presenta desafíos particulares debido a la naturaleza global de Internet, el anonimato que ofrece, los avances tecnológicos rápidos y la dificultad para identificar y enjuiciar a los delincuentes en línea. Además, la falta de programas de rehabilitación efectivos agrava esta situación. La naturaleza transfronteriza de Internet permite a los delincuentes seguir perpetrando delitos en jurisdicciones donde la ley es menos efectiva o donde encuentran cierto grado de protección. El anonimato en línea también reduce las capacidades de supervisión y puede aumentar la oportunidad de reincidencia (Nadolna & Rudenko, 2021).

Los ciberdelincuentes desarrollan habilidades técnicas para eludir las medidas de seguridad y continúan con sus actividades ilegales aprovechando el acceso a la tecnología y las oportunidades de autoformación en las redes sociales. Algunos ciberdelincuentes tienen la capacidad de ocultar sus huellas digitales, suplantar la ubicación y el correo electrónico de sus víctimas, y modificar rápidamente su perfil en línea, lo que les permite mantener múltiples identidades sin correr el riesgo de ser identificados como reincidentes (Curtis & Oxburgh, 2022).

La dificultad para enjuiciar a los delincuentes en línea se debe a la complejidad de las redes de ciberdelincuencia y la necesidad de una mayor coordinación internacional. Se requiere una respuesta multidisciplinaria que incluya capacitación especializada, asignación adecuada de recursos para la investigación y manejo de evidencia digital, así como la disponibilidad de programas de rehabilitación que aborden las complejidades del ciberdelito (Peters & Hindocha, 2020).

Para prevenir la reincidencia y disuadir a los delincuentes en línea, se han propuesto estrategias como el aumento de las sanciones y la cooperación internacional. Sin embargo, estas estrategias tienen limitaciones y pueden no ser efectivas en todos los casos. Las políticas de disuasión tradicionales, como la

amenaza de penas más severas, pueden no ser adecuadas para los ciberdelitos debido a la complejidad de la persecución y la lentitud de la investigación. Las sentencias por delitos cibernéticos a menudo no tienen en cuenta las diferencias entre el ciberdelito y el delito convencional, y es necesario desarrollar enfoques más sofisticados y completos para evaluar una variedad de factores y valorar el impacto en las víctimas (Choi & Toro-Álvarez, 2017).

En el caso del ciberdelito, el Departamento de Justicia de los Estados Unidos recomienda que los jueces sancionen a los ciberdelincuentes utilizando las Pautas de Sentencia (USSG), que tienen en cuenta diversos factores como la pérdida financiera de la víctima, el número de víctimas, la sofisticación de los medios utilizados, el riesgo de daño físico, el daño intencional y el acceso a infraestructura crítica. Sin embargo, la aplicación de estas pautas puede ser discrecional y varía en la práctica (Ahn, 2022).

La aplicación de los criterios de sentencia está precedida por quien es procesado y bajo qué criterios discrecionales son elegibles para ser encarcelados o puestos en libertad condicional (Young & Pearlman, 2022). Según el Departamento de Justicia de los Estados Unidos (2010), durante el período de cinco años del 2006 a 2010, un total de 1177 personas fueron condenadas y sentenciadas por delitos cibernéticos. De estos, solo el 51.7% (n = 608) recibió una sentencia que incluía algún tiempo de prisión. Para aquellos sentenciados a prisión, las sentencias fueron típicamente bastante cortas. De los que recibieron una pena de prisión, más de un tercio (34.9%) fue condenado a 12 meses o menos, el 27.3% recibió una pena de 13 a 24 meses de prisión, el 11.5% una pena de 25 a 36 meses, el 12.3% 37-60 meses y solo el 6.7% fueron condenados a más de 60 meses de prisión (Departamento de Justicia, 2010). Además, escasa información sobre las sentencias está disponible de manera pública y en algunos países estos documentos son de carácter reservado, y no existe investigación extensa en materia de disuasión del delito digital a partir de la aplicación de las sentencias.

Los datos anteriores sobre una pequeña porción de cibercriminales sentenciados a más de 60 meses de prisión visualizan una contradicción entre el aumento de las tasas de cibercrimen, el rigor de los criterios de sentencia y la aplicación de la pena entre los responsables de victimización en el ciberespacio. Siendo conscientes de la cantidad de delitos y conductas desviadas en el ciberespacio, concluir que tal contradicción es generalizable sería un error de grandes proporciones. Por tanto, un análisis concreto de un delito específico a partir de casos jurídicos reales nos permitirá delimitar el campo de reflexión e investigación y aportar datos reales base para futuras investigaciones en esta área de gran relevancia para una sociedad cada día más conectada a Internet.

Metodología

El presente estudio realizó un análisis documental incluyendo criterios de elegibilidad específicos, seleccionando fuentes de información de respaldo académico y científico, delimitando los sesgos de selección y sintetizando resultados acordes con los postulados de la metodología PRISMA en su versión 2020 (Lee & Koo, 2022).

Desde este marco, se enfocaron esfuerzos en estudiar casos penales disponibles en bases de datos especializadas, relacionados con procesos legales que involucraban el uso de medios digitales y MASI (material de abuso sexual infantil). Esta combinación de factores fue causal de inclusión y la falta de algunos de estos el criterio principal de exclusión. Otros criterios de exclusión contemplaron la duplicación del caso, información detallada de la sentencia, así como también la disponibilidad de información pública sobre el caso para ampliar detalles no presentes en la sentencia.

Como fuente de información principal, se utilizó la base de datos especializada en inglés *Case Law* asequible desde Google Académico en Estados Unidos de América. Es de anotar que *Case Law* no está disponible para países de habla hispana. Sobre este recurso de información, se incluyeron 37 documentos de manera preliminar, pero después de aplicar criterios de búsqueda con un riguroso proceso de selección para evitar duplicados y mejorar la calidad de la muestra final, la misma se redujo a 14 casos que cumplían con los criterios de interés de la investigación.

Entre los 37 documentos disponibles, cuatro de ellos se relacionaban con sentencias sobre casos de abuso infantil que no involucraron el uso del ciberespacio, 16 sentencias se relacionaron con jurisprudencia general con opiniones sobre casos relacionados con abuso infantil y pornografía sin identificar a los delincuentes o condenas individuales, y 17 documentos estuvieron relacionados con producción, posesión, distribución o fabricación de MASI. Estos documentos tenían información disponible sobre el caso, la persona sentenciada, los cargos y la sentencia presentada. Sin embargo, tres de estos documentos repetían información de otras sentencias analizadas con idénticos datos del mismo procesado y cargos penales, por lo que se seleccionó la muestra final de 14 casos (véase Tabla 1).

Tabla 1

Resumen de los documentos legales analizados (n = 14)

Caso	Cantidad de cargos	Descripción de los cargos	Sentencia
Davidson vs. Estado	205	Posesión de material que representa una actuación sexual de un niño.	75 años de prisión
Minch vs. Estado	48	Posesión o visualización de un asunto que represente una actuación sexual por parte de un menor, uso de un menor de dieciséis años en una actuación y abuso sexuales de un menor de doce años.	70 años de prisión
Groomes vs. Estado	21	Distribuir, poseer o ver material que represente una conducta sexualmente explícita que involucre a un niño.	63 años de prisión
Estado vs. Phelps	16	Explotación sexual de un menor.	45 años de prisión
Helton vs. Estado	10	Posesión de material que represente una actuación sexual por parte de un menor y distribución de material que represente una actuación sexual por parte de un menor.	20 años de prisión
Estado vs. Green	2	Recibir MASI.	120 meses de prisión y 5 años de libertad supervisada
Estado vs. Chiu	2	Recepción y posesión de MASI.	110 meses de prisión y cinco años de libertad supervisada
Estado vs. Wechsler	5	Recibir MASI.	87 meses de prisión
Estado vs. Dickson	No disponible	Producir, poseer, distribuir e intentar producir MASI.	384 meses
Morehouse vs. Estado	1	Distribución de MASI.	84 meses de prisión, seguidos de 15 años de libertad supervisada
Estado vs. Vance	10	Posesión de representaciones de un menor involucrado en conducta sexualmente explícita.	77 meses de encierro y 36 meses de custodia comunitaria
Estado vs. Knight	5	Posesión en primer grado de representaciones de un menor involucrado en conducta sexualmente explícita.	77 meses de prisión
Estado vs. O'neal	1	Posesión de MASI.	51 meses de prisión
Estado vs. Ferber	2	Violación de las leyes sobre la difusión de MASI.	45 días en prisión

Nota: la cantidad de cargos hace referencia a la cantidad de delitos procesados (Chawla, 2022).

Resultados

La comparación de los 14 casos y las guías de sentencia identificó que, de los ocho criterios definidos por la USSG, solo dos factores se aplicaron en más del 85% de casos. Esos criterios serían la "Evaluación de sofisticación de los medios" y el "Riesgo de muerte o lesiones". Respecto al primer criterio, 12 casos tuvieron en cuenta la evaluación de sofisticación de los medios para fijar la sentencia, un caso necesitó documentar mejor este criterio y un caso no incorporó este factor en su proceso de decisión. Por su parte, el criterio asociado con el riesgo de muerte o lesiones fue aplicado en la totalidad de los casos. Sin embargo, podemos observar que el rango de sentencias varió entre 45 días a 75 años en prisión y entre cinco y 15 años de libertad condicional.

Otros resultados significativos se relacionaron con los criterios "número de víctimas" y "daño intencional". Respecto al número de víctimas, solo el 14% de los casos trataron de aplicar este criterio, pero la complejidad del cibercrimen investigado requirió una justificación adicional. Es importante anotar que determinar la cantidad de víctimas en un caso de explotación infantil en línea, se requiere la aplicación de técnicas de investigación con mayor complejidad o con acceso a software especializado de alto costo. En la gran cantidad de casos con MASI, no fue posible identificar a las víctimas ni determinar que se trataba de la misma víctima en diferentes imágenes y videos.

Según Choi y Lee (2023), la técnica multimedia conocida como *morphing*, permite la manipulación de material multimedia transformando el color de la piel y otras características de la víctima, con lo cual se puede hipotetizar falsamente que son víctimas diferentes cuando en realidad es la misma persona.

El criterio de "daño intencional" visualizó una defensa por parte de los infractores respecto a ser consumidores de MASI y, por tanto, tratar de justificar que no eran responsables del daño que habría sufrido los niños. Sin embargo, cuatro casos sancionaron a los sospechosos por producción de esta clase de material, lo cual los relaciona con este criterio de manera directa.

Los cuatro criterios restantes, "conducta extraterritorial", "pérdida financiera", "tráfico de dispositivos de acceso" (es decir, información de cuentas bancarias, números de seguro social, contraseñas y otra información personal) y "acceso a infraestructuras críticas", no tuvieron una aplicación mayoritaria en los casos bajo análisis (véase Tabla 2).

La conducta extraterritorial, que es una de las características comunes del cibercrimen en su naturaleza transnacional, no tuvo mayor aplicación; por el contrario, el análisis del proceso de captura y procesamiento de los ciberofensores evidenció que tales procedimientos eran llevados a cabo por las autoridades locales y sin documentar intercambios internacionales de MASI. Este hallazgo invita a investigar más a fondo porque no existe el enfoque transnacional, aunque en el 57% de los casos, se les encontró a los cibercriminales procesados cientos de imágenes de MASI de diferentes procedencias en Internet.

Considerando las características de las víctimas, los criterios relacionados con la pérdida económica, de dispositivos de acceso, e ingreso a infraestructuras críticas no tuvo una correlación visible.

Tabla 2
Criterios de sentencia aplicados

Criterios	Aplicados	%	Requieren mayor documentación	%	No aplicados	%
Pérdida financiera	0	-	0	-	14	1.00
Número de víctimas	0	-	.14	-	-	-
Conducta extraterritorial	0	-	0	-	14	1.00
Evaluación de la sofisticación de los medios	12	.85	1	.07	1	.07
Tráfico de dispositivos o de elementos de acceso	0	-	0	-	14	1.00
Riesgo de muerte o lesiones	14	1.00	0	-	0	-
Daño intencional	4	.28	9	.64	1	.07
Acceso a infraestructura crítica	0	-	0	-	14	1.00

Fuente: Resumen de la aplicación de los criterios de sentencia.

Otro hallazgo de importancia identifica que solo en uno de los casos analizados (Estado vs. Green, 2021), la Corte estipuló el uso obligatorio de un *software* para monitorear la actividad del delincuente en un escenario de libertad supervisada. Este software es el programa de monitoreo/administración de Internet y computadoras (CIMP, por su nombre en inglés), que incluye funcionalidades de monitoreo para bloquear el acceso a Internet de una persona, filtrado de Internet, monitorear el uso de Internet y computadoras, monitorear las pulsaciones de teclas y capturar mensajes de texto, fotos, videos, llamadas, así como también el control y bloqueo de aplicaciones de terceros (Bailey, 2022).

Discusión de resultados

La restricción al uso de equipos bajo determinados sistemas operativos, como los teléfonos Android, trae consigo limitaciones operacionales de especial interés para la supervisión de los cibercriminales bajo libertad condicional, porque en algunos casos los infractores disponen de más de un dispositivo o están conectados mediante distintas plataformas y equipos de distintos fabricantes.

En el caso, Helton vs. Estado (2020), se encontró al delincuente en posesión de MASI en una computadora de escritorio, dos computadoras portátiles y tres teléfonos celulares. El enjuiciamiento de Jorden Knight (Estado vs. Knight, 2020), involucró la incautación de 322 archivos en una carpeta de almacenamiento en la nube pública en la plataforma Dropbox. El equipo de investigadores del caso Estado vs. Brown (2019) afirmó que nueve dispositivos estuvieron involucrados en el proceso de enjuiciamiento. Incluían una tableta Samsung, un Apple iPad Mini, un Microsoft Surface Pro, un Apple Macbook, un Google Pixel, un iPhone, un teléfono Motorola, una computadora de escritorio y una memoria USB.

Según Septianto y Mahawan (2021), se puede acceder a un pendrive desde múltiples dispositivos con acceso a Internet como un televisor, una videoconsola o un reproductor multimedia. Esta ampliación de la conexión a Internet y la visualización de MASI en múltiples dispositivos, añade complejidad a la supervisión de los infractores de libertad condicional y exige una definición de criterios con mayor especificidad para prevenir la reincidencia de los ciberdelincuentes.

Teniendo en cuenta lo anterior, el presente análisis permite explorar campos de acción en futuras investigaciones, que permitan delimitar los delitos y los criterios de comparación de las guías de la USSG. De igual forma, la identificación de diferentes jurisdicciones penales en cada Estado, invita a realizar investigaciones con

un mayor nivel de segmentación donde se comparen casos similares Estado por Estado, para comprender mejor el fenómeno antes de analizar los casos a nivel nacional.

Otra limitación para tener en cuenta, es el marco temporal de las sentencias. Es importante señalar que, entre los casos documentados, uno de ellos (Estado vs. Ferber, 1982), el individuo que recibió una sentencia de solo 45 días de prisión está relacionado con la facilitación de dos videos con material de abuso sexual infantil en 1982.

Finalmente, este ejercicio exploratorio puede brindar elementos orientadores para indagar sobre oportunidades de mejora, a partir de los casos documentados y la justificación del problema desarrollado en la primera parte de este documento. Haciendo hincapié en el escenario de permanente avance tecnológico y actualización de las técnicas cibercriminales, este documento invita a reflexionar sobre qué retos se pueden ver y afrontar desde una perspectiva innovadora y proactiva.

Conclusiones

El presente estudio concluye que las pautas de sentencia no se aplican completamente en los casos de delitos cibernéticos que involucran abuso infantil, lo cual requiere una investigación exhaustiva de cada caso para identificar factores decisivos en la sentencia. Estos factores incluyen la evaluación de la reincidencia, los antecedentes penales y la proximidad a las posibles víctimas. En el 50% de los casos analizados, se encontró que los delincuentes convivían con menores de edad, lo que indica que la reincidencia y la revictimización deben ser consideradas de manera más prominente en las condiciones de libertad condicional y supervisión. Sin embargo, la falta de información sobre estos escenarios requiere una investigación más amplia y un mejor proceso de documentación.

El análisis exploratorio de los 14 casos legales resumidos en este documento sugiere los siguientes puntos que deben abordarse mediante nuevas técnicas. Estos puntos incluyen mejorar la detección de los delitos cibernéticos, prevenir la victimización en línea secundaria y continua, aumentar la alfabetización sobre el alcance multiplicativo de los delitos cibernéticos, diseñar mecanismos de supervisión en línea que permitan la socialización controlada, involucrar terapias cognitivo-conductuales que incorporen el uso supervisado de las tecnologías de la información y la comunicación (TIC), y mejorar las capacidades para una adecuada gestión de la evidencia digital, especialmente en su recolección y tratamiento inicial.

La complejidad del delito y la victimización en el ciberespacio requiere que los esfuerzos de prevención y control del ciberdelito sean multidisciplinarios. Esto implica la participación de diferentes partes interesadas, incluidos los organismos encargados de hacer cumplir la ley, el sector privado y el público en general. Según Fonseca et al. (2023), la respuesta al laberinto que materializa la intervención del ciberdelito exige el desarrollo de nuevas herramientas y técnicas para combatir el ciberdelito en constante evolución.

La mejora de la detección del cibercrimen debe tener en cuenta que cada modalidad de delincuencia *online* tiene unas particularidades y una rentabilidad para el infractor. Por tanto, es importante estudiar los diferentes *modus operandi* y compartir dicho aprendizaje con los diferentes actores del sistema de justicia penal. Toro-Álvarez (2023) afirma que la evolución del ciberdelito debe motivar también una evolución en su investigación, detección y sanción. Nuevos mecanismos de monitoreo preventivo y alerta temprana en la distribución de MASI son requeridos, al igual que permitir la colaboración entre las diferentes instituciones a cargo de la aplicación de la ley y la persecución del delito. Los datos sobre el fenómeno del ciberdelito deben alimentar bases de datos compartidas que optimicen los procesos de toma de decisiones y contribuyan al análisis multidisciplinario de los éxitos y fracasos en el control del ciberdelito

Otra gran perspectiva de mejora es frenar la victimización *online* secundaria y permanente, y para ello, las instituciones pueden trabajar en la alfabetización sobre los alcances e impactos de la delincuencia *online* y la implementación de acuerdos de cooperación en Internet para la supresión de datos y el derecho al olvido. Wall (2008) documenta la importancia de los mecanismos de protección de datos,

especialmente para las víctimas donde se puede eliminar material no deseado de Internet y se protege el honor y el buen nombre de los afectados.

En cuanto a los métodos de supervisión para exconvictos bajo libertad condicional, es importante implementar mecanismos de vigilancia que no afecten las oportunidades de socialización y desarrollo personal que conlleva la interacción en Internet. Como lo documentan Choi et al. (2022), un equilibrio entre el monitoreo y la facilitación de oportunidades para solicitar empleo, educación y socialización y el monitoreo de un posible comportamiento desviado puede ayudar a reducir la reincidencia criminal. Aunque el programa de monitoreo de Internet (CIMP) es una herramienta que puede ayudar a controlar la navegación individual con fines ilícitos, es importante considerar que la conectividad puede darse por múltiples dispositivos, por lo que se requiere contar con una plataforma de vigilancia mucho más robusta que no dependa de la instalación en una computadora específica, pero que no se conviertan en un riesgo para los datos privados de los sujetos supervisados. Por ejemplo, tecnologías como Blockchain pueden abordar problemas de privacidad al tiempo que complementan las capacidades de auditoría y monitoreo (Toro-Álvarez & Motta-Castaño, 2017).

Los factores asociados con la supervisión son esenciales para disminuir la reincidencia, así como para motivar el comportamiento prosocial. Según Alford (2000), más allá de condenar y asegurar a una persona en una prisión bajo criterios disciplinarios exhaustivos, lo más importante es superar las limitaciones actuales de control y supervisión, dentro y fuera de las prisiones.

De la misma manera que los puntos calientes ubican geográficamente un área de alta incidencia criminal, se pueden mapear los puntos calientes de actividad cibercriminal (Lusthaus et al., 2020). Según las sentencias analizadas en este estudio, los investigadores capturaron a los delincuentes gracias a la implementación de herramientas de informática forense que rastreaba la información pública del sospechoso y las firmas digitales del MASI; esta información sigue estando disponible para los investigadores y puede extender su uso a las instituciones encargadas de la supervisión cuando el individuo se encuentra en libertad condicionada. Del mismo modo, esta georreferenciación de actividad cibercriminal permitiría identificar desde qué áreas hay un mayor comportamiento desviado en línea y poder intervenir con programas de promoción social, psicológica y profesional.

Según Hummer (2023), la incorporación de campañas de generación de conocimiento para incrementar las capacidades de gestión de evidencia digital, principalmente en su preservación y recolección inicial, es una estrategia que se puede implementar para reducir la reincidencia criminal al igual que acelerar los procesos investigativos y de sanción. La gestión y el intercambio de pruebas son cruciales para garantizar la aplicación de la ley y la regulación del delito cibernético y también pueden ayudar a mejorar las prácticas de supervisión cuando el procesado sale de prisión.

El incremento del cibercrimen, sus impactos, y la incorporación de mayores capacidades tecnológicas para delinquir y difundir material ilícito como MASI, requieren una innovación en las técnicas de investigación, procesamiento, control y monitoreo de las personas sentenciadas por delitos informáticos y cibercrimen. Tal innovación a su vez requiere una documentación rigurosa y una investigación científica que detecte las oportunidades de mejora y visualice la implementación exitosa o no, de ciertas políticas de control del delito que puede estar siendo aplicadas de manera parcial.

Las sociedades evolucionan en su forma de relacionarse, así como sucede con el comportamiento desviado humano en la actual cuarta revolución industrial; pero hay constantes que deben prevalecer en esas dinámicas, la protección de la niñez y de las víctimas, sin importar su condición o la clase de delito que les afecta, debe mantener la motivación para revaluar las prácticas de un sistema de justicia penal y su compromiso permanente con una sociedad más segura incluso en el ciberespacio.

Referencias

Ahn, M. J. (2022). Navigating beyond the lodestar: Borrowing the federal sentencing guidelines to provide fee-shifting predictability. *Dickinson Law Review*, *127*(1), 101-161. https://ideas.dickinsonlaw.psu.edu/dlr/vol127/iss1/4

Akhgar, B., & Brewster, B. (Eds.). (2016). *Combatting cybercrime and cyberterrorism. Challenges, trends and priorities*. Springer International Publishing Switzerland. https://doi.org/10.1007/978-3-319-38930-1

Alford, F. (2000). What would it matter if everything Foucault said about prison were wrong? Discipline and punishment after twenty years. *Theory and Society*, *29*(1), 125-146. https://doi.org/10.1023/A:1007014831641

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., …, & Zhou, Y. (2017). Understanding the mirai botnet. In *26th* [USENIX] *security symposium* ([USENIX] Security 17) (pp. 1093-1110).

Bailey, D. E. (2022). Emerging technologies at work: Policy ideas to address negative consequences for work, workers, and society. *ILR Review*, *75*(3), 527-551. https://doi.org/10.1177/00197939221076747

Bonnart, S., Capurso, A., Carlo, A., Dethlefsen, T. F., Kerolle, M., Lim, J., …, & Zarkan, L. C. (2023). Cybersecurity threats to space: From conception to the aftermaths. In *Space law in a networked world* (pp. 39-101). Brill Nijhoff.

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*, 102258. https://research.tue.nl/en/publications/cybercrime-threat-intelligence-a-systematic-multi-vocal-literatur

Chawla, A. (2022, October 24). *The rise of internet child pornography*. https://doi.org/10.2139/ssrn.4256854

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

Choi, K. S., & Toro-Álvarez, M. M. (2017). *Cibercriminología: Guía para la Investigación del Cibercrimen y Mejores Prácticas en Securidad Digital.* Fondo Editorial Universidad Antonio Nariño.

Choi, K., Back, S., & Toro-Álvarez, M. M. (2022). *Digital forensics & cyber investigation*. Cognella Academic.

Choi, K. S., & Lee, H. (2023). The trend of online child sexual abuse and exploitations: a profile of online sexual offenders and criminal justice response. *Journal of Child Sexual Abuse*, *16*(1), 1-20. https://doi.org/10.1080/10538712.2023.2214540

Choo, K. K. R. (2011). *Cybercrime: An overview of the legal challenges.* In Jaishankar, S. (Ed.). *Cyber criminology: Exploring Internet crimes and criminal behavior* (pp. 227-244). Routledge.

Curtis, J., & Oxburgh, G. (2022). Understanding cybercrime in 'real world'policing and law enforcement. *The Police Journal*, *0*(0), Ahead of Print. https://doi.org/10.1177/0032258X221107584

Departamento de Justicia de los Estados Unidos. (2010, December 17). PRO IP Act: *Annual Report 2010*. Washington, D.C.: Author. www.cyber crime.gov/proipreport2010.pdf

Dodge, C., & Burruss, G. (2019). Policing cybercrime: Responding to the growing problem and considering future solutions. In Leukfeldt, R., & Holt, T.J. (Eds.). *The human factor of cybercrime* (pp. 339-358). Routledge.

Estado v. Brown, No. 2: 18-CR-00037-FL-2 (D.N.C. July 26, 2019).

Estado v. Ferber, 458 U.S. 747, 102 S. Ct. 3348, 73 L. Ed. 2d 1113 (1982).

Estado v. Green, 954 F. 3d 1119 (8th Cir. 2020).

Estado v. Knight, No. 81837-6-I (Wash. Ct. App. Nov. 9, 2020).

Estado v. O'NEAL, 17 F.4th 236 (1st Cir. 2021).

Europol, E. C. C. (2021). *The Internet organized crime threat assessment (IOCTA).* European cybercrime center. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Fonseca, C. C., Moreira, S., & Guedes, I. (2023). The prevention and control of online consumer fraud. In Don Hummer, T & James, B. (Eds.). *Handbook on crime and technology* (pp. 395-410). Edward Elgar Publishing.

Frase, R. S. (2019). Sentencing guidelines in American courts: A forty-year retrospective. *Federal Sentencing Reporter*, *32*(2), 109-123.

Gillespie, A. A. (2015). *Cybercrime: Key issues and debates*. Routledge.

Helton v. Estado, 595 S. W. 3d 128 (Ky. 2020).

Holt, T. J. (2012). Exploring the intersections of technology, crime, and terror. *Terrorism and Political Violence*, *24*(2), 337-354. https://doi.org/10.1080/09546553.2011.648350

Hofer, P. J. (2019). Federal sentencing after Booker. *Crime and Justice*, *48*(1), 137-186.

Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge. https://doi.org/10.4324/9781315775944

Hummer, D. (2023). Techno-crime cause, prevention, and control: Issues to consider. In Don Hummer, T & James, B. (Eds.). *Handbook on crime and technology* (pp. 1-15). Edward Elgar Publishing.

Internet Crime Complaint Center. (2022). *Federal Bureau of Investigation Internet Crime (FBI).* https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics

Jones, T., & Newburn, T. (2002). Policy convergence and crime control in the USA and the UK. *Criminal Justice*, *2*(2), 173-203. https://doi.org/10.1177/17488958020020020401

Lee, H., & Wildeman, C. (2021). Assessing mass incarceration's effects on families. *Science*, *374*(6565), 277-281.

Lee, S. W., & Koo, M. J. (2022). PRISMA 2020 statement and guidelines for systematic review and meta-analysis articles, and their underlying mathematics: Life Cycle Committee Recommendations. *Life Cycle*, *2*(e9), 1-10. https://doi.org/10.1126/science.abj7777

Luknar, I. M. (2020). Cybercrime-emerging issue. *Archibald Reiss Days, Thematic Conference Proceedings of International Significance (Vol. 10, p. 621- 628). Beograd: Kriminalističko-policijski univerzite*

Lusthaus, J., Bruce, M., & Phair, N. (2020). Mapping the geography of cybercrime: A review of indices of digital offending by country. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 448-453). Conference paper.

Marcum, C. D., Higgins, G. E., & Tewksbury, R. (2011). Doing time for cybercrime: An examination of the correlates of sentence length in the United States. *International Journal of Cyber Criminology*,*5*(2), 824–835.

Moneva, A., Leukfeldt, E. R., & Romagna, M. (2023). Fieldwork experiences researching cybercriminals. In Díaz, A., Del-Real, C., & Molnar, L. (Eds.). *Criminology and security: Methods, ethics, and emotions*. (In press), Springer Nature.

Nadolna, M., & Rudenko, A. (2021). Interpol activities to coordinate cooperation to fight cybercrime. Topical issues of humanities. *Technical and Natural Sciences*, 299-302. https://jti.donnu.edu.ua/article/view/12014

Peters, A., & Hindocha, A. (2020, June 26). *US global cybercrime cooperation: A brief explainer.* Third Way. https://www.thirdway.org/memo/us-global-cybercrime-cooperation-a-brief-explainer

Samia, A. S. (2021). Crime and punishment in William Davenant's Macbeth: A stoic perception. *Journal of Early Modern Studies*, *10*, 151-171. https://doi.org/10.13128/jems-2279-7149-12545

Septianto, D., & Mahawan, B. (2021). USB flash drives forensic analysis to detect Crown Jewel data breach in PT. XYZ (coffee shop retail-case study). In *9th International Conference on Information and Communication Technology (ICoICT)* (pp. 286-290). IEEE.

Singh, M., Singh, M., & Kaur, S. (2019). Issues and challenges in DNS based botnet detection: A survey. *Computers & Security*, 86, 28-52. https://doi.org/10.1016/j.cose.2019.05.019

SonicWall. (2022). *Sonicwall cyber threat report*. https://acortar.link/SSgDh6

Stalans, L. J., & Horning-Ruf, A. (2023). Internet sex crimes. In *Handbook on crime and technology* (pp. 116-137). Edward Elgar Publishing.

Steinmetz, K. F., & Yar, M. (2019). Cybercrime and society. *Cybercrime and Society. SAGE Publications.*

Strasburger, V. C., Zimmerman, H., Temple, J. R., & Madigan, S. (2019). Teenagers, sexting, and the law. *Pediatric*s, *143*(5), e20183183. https://doi.org/10.1542/peds.2018-3183

Toro-Álvarez, M. M. (2023). Hacking. In Don Hummer, T & James, B. (Eds.). *Handbook on crime and technology* (pp. 334-357). Edward Elgar Publishing.

Toro-Álvarez, M. M., & Motta-Castaño, D. (2017). Articuladores de innovación social para contrarrestar amenazas a la seguridad ciudadana. *Revista Logos, Ciencia & Tecnología*, *8*(2), 24-34. https://doi.org/10.22335/rlct.v8i2.315

Tuan, T. A., Long, H. V., Son, L. H., Kumar, R., Priyadarshini, I., & Son, N. T. K. (2020). Performance evaluation of Botnet DDoS attack detection using machine learning. *Evolutionary Intelligence*, 13, 283-294.

Wall, D. S. (2008). Cybercrime, media, and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology*, *22*(1-2), 45-63. https://ssrn.com/abstract=1124662

Young, K. M., & Pearlman, J. (2022). Racial disparities in lifer parole outcomes: The hidden role of professional evaluations. *Law & Social Inquiry*, *47*(3), 783-820. https://doi.org/10.1017/lsi.2021.37