Quórum Legislativo
Núm. 142, junio 2023, 75-105

CIBERSEGURIDAD Y CIBERDELINCUENCIA. REGULACIÓN VIGENTE Y PENDIENTES LEGISLATIVOS EN MATERIA DE ROBO DE IDENTIDAD Y FRAUDE

CYBERSECURITY AND CYBERCRIME. CURRENT AND PENDING LEGISLATION ON IDENTITY THEFT AND FRAUD

Israel PALAZUELOS COVARRUBIAS[1]

RESUMEN: Con el objetivo de identificar los más recientes hallazgos acerca del robo de identidad y fraude cibernéticos, se lleva a cabo una meta-revisión sistemática de la literatura científica bajo criterios de utilidad en el ámbito legislativo mexicano, la que conduce a apreciar la necesidad de armonización jurídica con los estándares internacionales (claridad, precisión y actualización), así como de un conjunto de herramientas avanzadas para enfrentar dichos ciberdelitos. De acuerdo con los textos revisados, estos aspectos deberían ser considerados en cualquier marco regulatorio en materia de ciberseguridad y ciberdelincuencia, con el objetivo de reducir la criminalidad cibernética, identificarla, perseguirla y castigarla para evitar la impunidad y proteger a los usuarios en su identidad, patrimonio e integridad.

PALABRAS CLAVE: Legislación cibernética, ciberdelitos, revisión sistemática, herramientas forenses, criptomonedas, Inteligencia Artificial.

ABSTRACT: To identify the most recent findings about identity theft and cyber fraud, a systematic meta-review of the scientific literature is carried out under criteria of utility in the Mexican legislative sphere, which leads to an appreciation of the need for legal harmonization with international standards (clarity, precision, and updating), as well as a set of advanced tools to deal with such cybercrimes. According to the revised texts, these aspects should be considered in any regulatory framework on cybersecurity and cybercrime, with the aim of reducing the commission of cybercrime, identifying, pursuing, and punishing them to avoid impunity and protect users in their identity, heritage, and integrity.

KEYWORDS: Cyber legislation, cybercrime, systematic review, forensic tools, cryptocurrencies, Artificial Intelligence

1 Investigador A del Centro de Estudios de Derecho e Investigaciones Parlamentarias de la Cámara de Diputados, maestro en Ciencia Política por la Universidad de Salamanca.

SUMARIO: I. *Introducción.* II. *Diseño de la revisión sistemática.* III. *Resultados: Evidencia sobre ciberseguridad y ciberdelincuencia.* IV. *Discusión: Utilidad en el ámbito legislativo mexicano.* V. *Conclusiones.* VI. *Referencias.*

I. INTRODUCCIÓN

La seguridad en ambientes tecnológicos es un tema relativamente nuevo que requiere de atención debido a la vulneración de la que personas usuarias son objeto. En este contexto, el robo de identidad y fraude cibernéticos son delitos recurrentes y de los que más daño patrimonial causan. Por ello, es indispensable que la población y sus representantes se hagan de los medios necesarios para combatirlo desde todos los frentes posibles, incluido el legislativo.

El robo de identidad y el fraude se producen cuando los datos personales de un individuo se obtienen ilegalmente y se utilizan posteriormente para, por ejemplo, conseguir créditos, abrir cuentas bancarias, comprar mercancías y acumular deudas (incluso millonarias) a nombre de las víctimas, cometiendo suplantación y uso indebido de documentos.[2] El carácter cibernético o virtual se encuentra definido, precisamente, por los medios a través de los que se cometen.

Las redes criminales sofisticadas están utilizando el ciberespacio para cometer nuevos delitos contra las personas usuarias que llevan a cabo sus actividades cotidianas de manera virtual en este entorno. Con ello, se pone a prueba la capacidad de los legisladores para regular eficazmente este ámbito toda vez que operan en un entorno multijurisdiccional, lo que dificulta el seguimiento y enjuiciamiento de estos delincuentes,[3] además de que es un problema cuyas particularidades (como su *modus operandi*) mutan rápidamente.

Es de suma importancia que los países cuenten con una regulación integral sobre delitos cibernéticos, alineada con los estándares internacionales, con la que se tomen medidas para reducir la brecha digital y aumentar la conciencia sobre seguridad cibernética entre

2 CASSIM, Fawzia, "Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?", *Potchefstroom Electronic Law Journal 18*, núm. 2, 2015, pp. 69-110.

3 *Idem.*

países y su población usuaria.[4] En particular, se requiere de un enfoque de desarrollo flexible, adaptable y ágil desde el marco regulatorio.[5]

Dada la naturaleza y rapidez con la que evoluciona este fenómeno, configura un problema público que reta sustantivamente al Poder Legislativo y que invita a que sus acciones adopten los estándares internacionales en la materia, así como la evidencia científica con la que se cuenta. Por ello, este documento pretende reunir tales insumos teniendo como base a las investigaciones arbitradas más recientes.

En suma, se sabe que existen diversos elementos tanto técnicos como empíricos que pueden ayudar a legisladores y legisladoras a enfrentar y aminorar el problema de la ciberdelincuencia, que además pudieran ser considerados en el debate público dada la evidencia que existe en cuanto a su efectividad.

De esta manera, el objetivo de la presente investigación es analizar y evaluar los hallazgos existentes en la literatura científica sobre la adopción de medidas legales efectivas para combatir la ciberdelincuencia, específicamente las relacionadas con el robo de identidad y fraude, así como extraer insumos desde la experiencia internacional que se consideran relevantes y útiles para los trabajos legislativos en México, en función de la evidencia disponible.

Como se verá, el grueso de investigaciones está orientado o por lo menos cuenta con elementos a comprobar que la atención efectiva desde el Poder Legislativo, en cuanto al establecimiento de disposiciones que empleen los elementos técnicos y estándares internacionales sobre seguridad cibernética, reduce significativamente el riesgo de sufrir delitos de esta índole por parte de las personas usuarias.

Este documento se desarrolla en tres partes principales: en la primera, luego de esta introducción, se describe la manera en que se diseñó la meta-revisión; en seguida se presentan los resultados sobre la evidencia que existe sobre el tema; lo que conduce, finalmente, a un planteamiento sobre la potencial utilidad en el ámbito legislativo mexicano.

4 *Cfr*. CHANG, Lennon, "Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia", en HOLT, Thomas y BOSSLER, Adam (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Palgrave Macmillan, Cham, 2020, pp. 327-343.

5 *Cfr*. SKIAS, Dimitrios *et al.,* "Demonstration of Alignment of the Pan-European Cybersecurity Incidents Information Sharing Platform to Cybersecurity Policy, Regulatory and Legislative Advancements", en *ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security*, Nueva York, Association for Computing Machinery, 2022, pp. 1-8.

II. DISEÑO DE LA REVISIÓN SISTEMÁTICA

Existen diversas definiciones de lo que es una Revisión Sistemática de Literatura (RSL) en el ámbito de la investigación científica. Inicialmente, se puede afirmar que la RSL es una metodología ampliamente empleada, de gran utilidad para sintetizar y sistematizar la evidencia que existe sobre un tema en particular, bajo determinados criterios, ante una gran cantidad de publicaciones. Se enfoca en identificar, seleccionar y evaluar críticamente todos los estudios relevantes publicados con el fin de responder una o más preguntas específicas de investigación, así como de proporcionar una síntesis sistemática y objetiva que sea de utilidad, en este caso, para el ámbito legislativo.

De acuerdo con diversos autores, la RSL crea una base firme para avanzar en el conocimiento y facilita el desarrollo de la teoría, identificando aspectos del tema en los que existe abundante material y descubriendo áreas en las que es necesario comenzar a investigar o, en su caso, seguir investigando.[6] Además, algo que es de sumo interés para los fines de este trabajo, es que se considera un procedimiento científico que aporta evidencia de alto nivel en la toma de decisiones.[7]

La RSL se configura en un estudio detallado, selectivo y crítico que integra la información esencial en una perspectiva unitaria y de conjunto,[8] cuya finalidad es examinar la bibliografía publicada y situarla en cierta perspectiva.[9] En ella, el revisor recoge datos a partir de los artículos, los analiza y extrae una conclusión.

A pesar de que la RSL representa múltiples beneficios para el conocimiento, esta es poco recurrida en los estudios provenientes del ámbito legislativo, probablemente por el tiempo que conlleva llevarla a cabo, frente del que se dispone. Sin embargo, bajo los procedimientos estándares de esta metodología, podría hacerse una adaptación tal que no comprometa la calidad de los resultados, se logre llevar a cabo en un breve periodo y sea de utilidad para el ámbito legislativo. En esta

6 *Cfr*: WEBSTER, Jane y WATSON, Richard T., "Analyzing the Past to Prepare for the Future Writing a Literature Review", *MIS Quarterly*, 26-2, 2002, p. 13.

7 Véase FETTKE, Peter, "State of the Art des State of the Art Wirtschaft" *Informatik,* 48-257, 2006.

8 ICART ISERN, María Teresa y CANELA SOLER, Jaume, "El artículo de revisión", *Enferm Clin*, 4(4), 1994, pp. 180-184.

9 RAMOS, Miguel H. *et al.*, "Cómo escribir un artículo de revisión", *Revista de postgrado de la VI Catedra de Medicina*, 2003, p. 126.

investigación se propone una modalidad que se encuentra detallada a continuación.

Cabe advertir que este trabajo se configura en una revisión sistemática de diferentes RSL, o sea, que dicha adaptación inicia por llevar a cabo una meta-revisión de la literatura en la que se seleccionan las publicaciones que, cumpliendo con todos los criterios previstos, hayan revisado fuentes primarias, lo cual permite abarcar de manera indirecta numerosas investigaciones que en conjunto emplean una amplia variedad de metodologías, enfoques y áreas de estudio.

Las preguntas de investigación que permiten cumplir con los objetivos de este trabajo son:

- ¿Qué hallazgos hay en la literatura científica en materia de adopción de medidas legales efectivas para el combate a la ciberdelincuencia, particularmente del robo de identidad y fraude?
- ¿Qué preceptos normativos ha previsto la comunidad internacional (otros países del mundo) y cuáles se considera importante adoptar dada la evidencia que existe?

Teniendo en cuenta lo anteriormente vertido, se describe el diseño de la meta-revisión sistemática, incluyendo los criterios de inclusión y exclusión de las publicaciones, las estrategias de búsqueda utilizadas, los métodos de selección y evaluación de los estudios, así como los métodos de síntesis de los resultados.

1. *Base de datos y motor de búsqueda*

La base de datos que se emplea es *Scopus*, una de las más amplias a nivel global sobre literatura revisada por pares, la que incluye revistas científicas, libros y actas de congresos. Contiene arriba de 21,900 títulos de más de 5,000 editoriales de todo el mundo, en el campo de la ciencia, tecnología, ciencias sociales y otras. Esta base cuenta con 54 millones de registros que datan de 1823, 84% de los cuales se publicaron a partir de 1996.[10]

Cabe decir que, a pesar de emplear únicamente este recurso como punto de partida (y recordando que se lleva a cabo una meta-revisión de la literatura), cada investigación analizada, al configurarse en RSL, conjuntan diversas bases y motores de búsqueda, con lo que

10 ELSEVIER, *Scopus. Guía rápida de referencia*, (12 de junio de 2023), https://www.recursoscientificos.fecyt.es/sites/default/files/guia-del-usuario.pdf.

se alcanzan varias otras de manera indirecta, como se describe en las siguientes páginas.

2. *Criterios de inclusión y exclusión*

A continuación, se especifican los criterios de inclusión y exclusión de las publicaciones que se tuvieron en cuenta para llevar a cabo el análisis planteado.

A. *Temporalidad*

Dada la naturaleza del fenómeno, principalmente en cuanto a sus rápidos cambios, se privilegia la selección de las investigaciones más recientes, es decir, las publicadas entre enero de 2020 y mayo de 2023.

B. *Ámbito geográfico*

El propio tema de la ciberseguridad y los objetivos de esta investigación hacen necesario no limitar la selección mediante este criterio, por el contrario, es de sumo interés conocer experiencias de todo el mundo que pudieran ser aprovechadas en México.

C. *Idioma*

Se hizo un filtro para incluir solo aquellas investigaciones escritas en inglés, español o portugués. Con las características deseadas, casi la totalidad de las publicaciones son en el idioma inglés y solo una en español.

D. *Tipo de documentos*

Únicamente se incluyen las RSL que hayan sido publicadas en revistas científicas con revisión por pares, con la finalidad de incluir indirectamente un mayor número de estudios de todo el mundo, que hayan sido analizados rigurosamente. Es precisamente esta característica la que define a la presente investigación como una meta-revisión de una selección de publicaciones confiables y valiosas.

E. *Materia*

No se delimitó materia o área científica alguna, esto con la finalidad de reunir una visión multidisciplinaria del fenómeno y al mismo tiempo conocer en cuáles de ellas se inscribe la literatura resultante, asimismo, de manera particular, definir si es útil o no para este estudio, pero no con base en el área.

3. *Estrategia de búsqueda*

La búsqueda se realizó mediante una ecuación, misma que fue introducida en el motor de la propia base de datos empleada (*Scopus)*. Esta se orientó a los títulos, palabras clave y resúmenes de las publicaciones la que, con la ayuda de operadores *booleanos*, se conformó de tres elementos con un conjunto de palabras cada uno: El primero es relativo al delito o delitos de interés para este estudio (robo de identidad y fraude), así como sus sinónimos (defraudación, usurpación, suplantación, etc.). El segundo define, ya sea el entorno en que se comete el delito (en línea, internet, ciberespacio) o la materia en la que se halla (ciberseguridad o ciberdelincuencia). El tercero agrega el componente legislativo o legal (también junto con distintos sinónimos y palabras derivadas) de tal forma que se ciña o al menos se relacione explícitamente a este ámbito.

Dicha estrategia asegura, al mismo tiempo, que los trabajos resultantes traten o al menos hagan referencia a los ciberdelitos de interés para esta investigación (robo de identidad y/o fraude); que dichos crímenes en un ambiente físico o *tradicional* no sean su enfoque principal; y que tenga en cuenta el aspecto legal o legislativo de manera expresa.

4. *Filtros*

Cada uno de los filtros empleados se ha descrito con anterioridad, el resto se aplica a juicio del investigador con base en la orientación del contenido de cada publicación, buscando que estas se enfoquen en las personas usuarias, más que en instituciones u organizaciones.

5. *Análisis*

De cada texto resultante se extrae una o más *lecciones* o *aportaciones* propicias para ser consideradas en nuestro país, con la seguridad de que son producto de investigaciones científicas revisadas por pares, como se aludió arriba. Al mismo tiempo, se trata de explicar su posible beneficio.

Como se verá en seguida, la presentación del análisis procura brevedad, así como un orden tal que vaya de lo general a lo particular. Se inicia por la delimitación de los delitos, hasta llegar a aspectos técnicos muy concretos como lo es el análisis forense del tema.

III. RESULTADOS: EVIDENCIA SOBRE CIBERSEGURIDAD Y CIBERDELINCUENCIA

En este apartado se da cuenta de los resultados de la meta-revisión. Así, los hallazgos más recientes en la materia se presentan a través de una descripción de los estudios incluidos, cuyo contenido resalta el o los componentes de mayor interés para el ámbito legislativo.

Siguiendo el procedimiento descrito en el apartado anterior, se tuvo un resultante de 16 artículos revisados por pares y publicados en revistas listadas en la base de datos que se empleó. De estos, con la finalidad de tener un cúmulo de publicaciones desde las cuales llevar a cabo el análisis a profundidad, se seleccionaron 10 que, por ser de principal interés para el presente trabajo, tienen como unidad de análisis a personas usuarias (o que al menos se enfoca en afectaciones hacia ellas), dejando de lado las que se centran en organizaciones.

Los trabajos finalmente seleccionados se explican a continuación.[11] En la Tabla 1, se enlista cada uno de ellos, se dispone al inicio con la intención de que funcione como resumen e índice de lo que el lector encontrará a lo largo del apartado. En conjunto se trata de investigaciones muy recientes, cuyas autoras y autores se encuentran adscritos a diferentes instituciones en el mundo. Todos los textos se encuentran publicados en revistas indexadas que editan importantes instituciones (Tabla 1).

11 Como se ve a lo largo de este documento, este grupo de textos se emplea como base del análisis dada su naturaleza y por ser resultado de la adaptación metodológica de la meta RSL de la que se dio cuenta, no obstante, se hace uso de diferentes fuentes complementarias.

Tabla 1. Artículos analizados sobre ciberseguridad y ciberdelincuencia por tema principal y datos de publicación.

	Autoría y año de publicación	Tema principal	Revista (país) y editor
1	Mayer Lux y Oliver Calderón, 2020	Concepto y delimitación de *fraude informático*	*Revista Chilena de Derecho y Tecnología* (Chile), Universidad de Chile
2	Khan *et al.*, 2022	Legislación sobre ciberdelincuencia	*F1000 Research* (Reino Unido), *F1000 Research*
3	Guo *et al.*, 2021	Contramedidas del fraude en línea	*IEEE Access* (Estados Unidos), *Institute of Electrical and Electronics Engineers Inc.*
4	Bisht *et al.*, 2022	Perspectiva tecnológica de la digitalización en las finanzas de las empresas	*Electronics* (Suiza), *Multidisciplinary Digital Publishing Institute (MDPI)*
5	Kushnirenko y Kharatishvili, 2022	Criminalidad con criptomonedas y análisis forense	*Kutafin Law Review* (Rusia), *Kutafin Moscow State Law University (MSAL)*
6	Choithani *et al.,* 2022	Inteligencia Artificial y ciberseguridad en criptomonedas y el sistema bancario	*Annals of Data Science* (Alemania), *Springer Science and Business Media Deutschland GmbH*
7	Mambile y Mbogoro, 2020	Delitos cibernéticos, leyes cibernéticas y su práctica en el sector público	*International Journal of Advanced Technology and Engineering Exploration* (India), *Accent Social and Welfare Society*
8	Barker, 2020	Concientización y educación a los clientes sobre la prevención del fraude en la banca electrónica	*South African Journal of Business Management* (Sudáfrica), *AOSIS (Pty) Ltd*
9	Jeyanthi *et al.*, 2020	Análisis de fraude en los sectores bancarios	*Journal of Critical Reviews* (India), *Innovare Academics Sciences Pvt. Ltd*
10	Fernandes y Antunes, 2023	Análisis forense digital	*Forensic Science International: Digital Investigation (Reino Unido), Elsevier Ltd.*

Fuente: Elaboración propia.

Las descripciones que se encuentran a continuación tratan de seguir un orden tal que los trabajos más amplios, o con temas más generales, se presentan al inicio; los textos que se enfocan en un aspecto mucho más particular en segundo lugar; y finalmente, un grupo de investigaciones que se centran en países que no necesariamente se destacan por encontrarse a la vanguardia en el tema, pero que, sin embargo, de estos también se rescatan varios aspectos que resultan útiles de acuerdo con los objetivos planteados.

Combinando un análisis doctrinal y legal en el contexto chileno, el trabajo de Mayer Lux y Oliver Calderón[12] analiza al fraude informático como un delito que, para lograr su correcta tipificación, necesita ser delimitado mediante la especificación de sus características y la diferenciación de otras conductas delictivas con cierta similitud, como el espionaje o el sabotaje cibernéticos. Dicha investigación, como se verá, ayuda a tener claridad en cuanto a lo que es el fraude cibernético, así como de la necesidad de regulación en aquel país sudamericano y en el mundo, iniciando, precisamente, por la definición del delito.

El análisis que tiene como base al Convenio de Budapest, del que Chile es parte desde 2017, hace énfasis en que la incorrecta delimitación de dichos delitos cibernéticos representa una dificultad en su regulación. En el caso particular del fraude, los autores consideran que comúnmente se incluyen dentro de su noción "conductas que en realidad corresponden a etapas de ejecución imperfecta a (delito tentado o frustrado) e incluso a actos preparatorios de un fraude propiamente [o bien], a conductas que en verdad corresponden a otros delitos informáticos […]"[13]

Con base en lo señalado, el trabajo plantea la necesidad de una reforma legislativa que tipifique el fraude cibernético como un delito con tres características definitorias:

> […] primero, la verificación de la conducta típica consistente en «manipular» datos o programas de sistemas de tratamiento automatizado de la información; segundo, la provocación de un resultado típico, que se identifica con un «perjuicio patrimonial» ajeno; y, tercero, la presencia de «ánimo de lucro» en el agente del comportamiento incriminado.[14]

Los autores hacen énfasis en que los tres requisitos que definen al delito deben presentarse juntos para poder afirmar jurídicamente que se trata de tal conducta. Con ello, desde luego, acompañarlo de una sanción, la que consecuentemente podrá ser aplicada sin poner en

12 MAYER LUX, Laura y OLIVER CALDERÓN, Guillermo, "El delito de fraude informático: concepto y delimitación", *Revista Chilena de Derecho y Tecnología* 9, núm. 1, 2020, pp. 151-185, https://www.scielo.cl/pdf/rchdt/v9n1/0719-2584-rchdt-9-1-00151.pdf.

13 *Ibidem*, p. 179.

14 *Idem.*

tela de juicio de si se trata, o no, de fraude cibernético y evitar así la impunidad del comportamiento.

La revisión de Khan *et al.,*[15] en la que intervienen seis personas autoras, todas ellas de la Universidad Multimedia de Malasia, analiza 72 textos provenientes de siete bases bibliográficas.[16] Es una de las pocas investigaciones recientes que aborda el tema directamente a través de la legislación como elemento principal para hacer frente a los ciberdelitos, incluidos los de robo de identidad y fraude, además de que es una de las más amplias.

El trabajo observa que el incremento en el número de delitos cibernéticos va acompañado de un aumento en el nivel de sofisticación de la tecnología empleada, lo que produce vulneraciones de seguridad y pérdidas importantes en contra de individuos, organizaciones y naciones.

Ante ello, los autores consideran que, además de que la legislación es débil debido a la existencia de múltiples lagunas, hay una falta de campañas de sensibilización y prevención, lo cual no abona en la disuasión de los ataques y, por ende, propicia que los delincuentes sigan cumpliendo con su cometido.

Identifican al Convenio de Budapest como el primer y único instrumento internacional vinculante sobre el delito cibernético que también sirve como una guía básica para cualquier país que esté desarrollando legislación para combatirlo, además de que proporciona una solución integral, operativa y funcional para la investigación y el enjuiciamiento del delito cibernético tanto a nivel nacional como entre las Partes firmantes.[17]

Junto con ello, identifican una serie de tratados y acuerdos internacionales sobre ciberdelincuencia, así como de leyes modelo, lo que se configura en un conjunto de instrumentos jurídicos al alcance de las naciones en el mundo, incluida la mexicana, que funcionan como insumos para el desarrollo de legislación en la materia (Tabla 2).

15 KHAN, Shereen *et al*., "A systematic literature review on cybercrime legislation", *F1000 Research* 11, núm. 971, 2022, pp. 1–18, https://doi.org/10.12688/f1000research.123098.1.

16 A saber, *ACM Digital Library, Emerald, Hein Online, ProQuest, ScienceDirect, Scopus* y *Westlaw Asia.*

17 *Cfr.* KHAN, Shereen *et al*., *op. cit.,* pp. 7 y 8.

Tabla 2. Tratados internacionales y leyes modelo sobre ciberseguridad y ciberdelincuencia.

	Instrumento	Descripción / utilidad
1	Tratados del Consejo de Europa: Convenio sobre la Ciberdelincuencia (2001) (Convenio de Budapest)	Primer acuerdo internacional para reducir el ciberdelito mediante la armonización con las leyes nacionales, mejorar las técnicas de investigación y aumentar la cooperación internacional.
2	Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (2003)	Ampliación del alcance del Convenio de Budapest para cubrir los delitos de propaganda racista o xenófoba.
3	Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (2000) (Convención de Palermo)	A pesar de no abordar explícitamente el delito cibernético, obliga a las partes a promulgar leyes para la cooperación en materia de extradición [aspecto esencial en la persecución de estos delitos dada su naturaleza multi jurisdiccional].
4	Convención sobre los Derechos del Niño (1989)	Protección de los Estados Parte al niño(a) de todas las formas de explotación y abuso sexual, incluidas la prostitución y la pornografía (Artículo 34).
5	Protocolo Facultativo de la Convención sobre los Derechos del Niño (2001)	Prohíbe la pornografía infantil y menciona Internet como medio de distribución.
6	Convención para la Protección de los Niños contra la Explotación y el Abuso Sexual (2007)	La Convención tipifica como delito la captación de niños con fines sexuales (*grooming*) y el turismo sexual.
7	Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales (2014)	Aborda (i) las transacciones electrónicas, (ii) la protección de datos personales, así como (iii) la ciberseguridad y el ciberdelito.
8	Ley Modelo de la Commonwealth sobre Delitos Informáticos y relacionados	Ayuda a los países de la *Commonwealt*h a mejorar el marco legal del delito cibernético en la criminalización e investigación de delitos informáticos y relacionados con la informática.
9	Ley Modelo sobre Ciberdelincuencia / e-crimen: Directrices de políticas modelo y textos legislativos (países del caribe)	Sincronización de la legislación, las políticas y los procedimientos que se relacionan con las Tecnologías de la Información y las Comunicaciones.
10	Ley Modelo Regional de Delitos Cibernéticos de las Islas del Pacífico	Se centra en el desarrollo de capacidades y de un marco normativo. Proyecto de la Unión Internacional de Telecomunicaciones y la Comisión Europea
11	Ley Modelo de la Comunidad de África Meridional para el Desarrollo (SADC)	Se centra en delitos informáticos y ciberdelincuencia.

Fuente: KHAN *et al.,*[18] traducción y adaptación propias a partir de sus Tablas 4 y 5.

18 *Idem*.

Los autores consideran que, por medio de estos y otros instrumentos, "todos los países deberían aspirar a seguir una política criminal común para disuadir a los ciberdelincuentes de manera efectiva mediante la coordinación, de tal manera que se facilite la detección del ciberdelito, la recopilación de pruebas, la investigación y, finalmente, el enjuiciamiento del caso con éxito".[19]

Con ello, advierten la necesidad de que cada país cuente con una legislación especializada y actualizada para tipificar el delito cibernético y otorgar facultades procesales suficientes para investigarlo, en la que además se tengan en cuenta a los diversos actores, se incluya la capacitación constante y el equipamiento con base en los últimos avances tecnológicos; se involucre a las autoridades encargadas de hacer cumplir la ley y a los proveedores de servicios de internet como cooperadores clave en la detección, prevención y respuesta a los delitos cibernéticos.

De igual manera advierten la necesidad de "cubrir una lista extensa de delitos cometidos en el ciberespacio, ya que algunas jurisdicciones se enfocan solo en delitos cibernéticos selectivos";[20] como el robo de identidad y fraude, considerados delitos tradicionales que se cometen ahora mediante la tecnología son tipificados comúnmente de manera genérica como *delitos cibernéticos*, lo cual consideran una inconveniencia.

En suma, sus resultados apuntan a que, ante el rápido avance de la tecnología, las leyes sobre ciberdelincuencia deben ir a la vanguardia mediante la cooperación entre naciones, particularmente a través de la incorporación de los preceptos provenientes del marco legal internacional en la legislación de cada uno de los países, de tal forma que se armonice y haga efectiva la persecución de este tipo de delitos.

El trabajo de Guo *et al.*,[21] por su parte, se configura en una extensa investigación en la que intervinieron seis autores y autoras adscritos en su mayoría al Departamento de Ciencias de la Computación del *Virginia Tech*,[22] Estados Unidos, en la que abordan múltiples inquietudes en torno al tema del engaño social en línea, así como sus contramedidas, es decir, maneras de enfrentarlo.

19 *Ibidem,* p. 8, traducción propia.

20 *Ibidem,* p. 12, traducción propia.

21 GUO, Zhen *et al.,* "Online Social Deception and Its Countermeasures: A Survey", *IEEE Access* 9, 2021, pp. 1770-1806, https://doi.org/10.1109/ACCESS.2020.3047337.

22 Instituto Politécnico y Universidad Estatal de Virginia.

La parte del trabajo que resulta de mayor interés para los objetivos propios tiene que ver con preocupaciones legales y éticas relacionadas con la investigación policial que se lleva a cabo sobre este tema (en términos genéricos), así como mecanismos técnicos, como los *honeypots,*[23] para obtener información de las personas atacantes y sus métodos.

La preocupación de las y los autores se centra en el hecho de que estas formas de acercamiento al problema se ponen en contacto con *usuarios humanos* o personas reales (víctimas o incluso atacantes) cuya información puede quedar expuesta, violando así su privacidad y, por ende, cometiendo un delito a pesar de sus intenciones meramente investigativas.

Los autores concluyen que no hay suficiente evidencia, mucho menos un consenso, acerca de qué metodologías deben permitirse y qué nivel de privacidad del usuario es necesario preservarse antes de lograr sus objetivos investigativos con fines de defensa.[24] Por ello, el trabajo conduce a afirmar que "deberían existir directrices y normas más específicas y claras a disposición de los investigadores"[25] para que tengan un marco legal bajo el cual desarrollar su labor.

En este mismo trabajo se hace una comparación entre los comportamientos fraudulentos fuera de línea (para los que la legislación se encuentra más desarrollada) y los que se suscitan en línea. Los autores subrayan que hay importantes similitudes, diferencias y, a su vez, conexiones.

> Muchas características del engaño fuera de línea tienden a observarse fácilmente en los comportamientos de engaño en línea. Sin embargo, debido al tiempo real o a las interacciones limitadas para sentir la presencia de las personas en las plataformas en línea […], algunas señales fisiológicas o psicológicas pueden no ser aplicables para detectar el engaño social en línea. Además, al detectarse el engaño, un engañador puede salir fácilmente de la situación en línea, mientras que un engañado puede perder fácilmente el rastro del engañador."[26]

23 De acuerdo con los autores, se puede decir que los *honeypots* son herramientas de seguridad informática empleadas "como un engaño defensivo para tratar proactivamente a los atacantes atrayéndolos a ellos y así evitar que accedan a un objetivo".

24 *Cfr.* GUO, Zhen *et al., op. cit.,* p. 1801.

25 *Ibidem*, p. 1798, traducción propia.

26 *Ibidem*, p. 1776, traducción propia.

Por ello, se destaca que también hacen falta leyes que consideren el incremento de la gravedad y frecuencia de los engaños cibernéticos, así como que a menudo estos conducen a delitos fuera de la red. La legislación en la materia debe considerar esa transición entre el origen virtual o cibernético del delito y su conclusión en un ambiente físico o real, incluso viceversa, pero a su vez diferenciar los comportamientos fraudulentos en línea y fuera de línea.

El trabajo de Bisht *et al.,*[27] tiene en cuenta la detección de fraude cibernético, específicamente en el sector financiero, mediante la incorporación de distintas tecnologías de la Industria 4.0 como el internet de las cosas, el *big data,* la automatización de procesos robóticos, el *blockchain*, entre otras. Esta investigación conjunta a nueve autoras y autores adscritos a universidades de India, México, España, Estados Unidos, Angola y Sudáfrica, quienes tienen en cuenta 61 estudios en la materia para llevar a cabo su revisión sistemática.

De acuerdo con las y los autores, dichas tecnologías deben ser integradas en el sector para mejorar la calidad, accesibilidad y seguridad de sus productos y servicios, no obstante, dentro de los problemas legales y regulatorios que identifican, principalmente en cuanto a la necesidad de su actualización, se encuentran los que "van desde la interoperabilidad y la disponibilidad del espectro hasta la ciberseguridad y la privacidad".[28]

El trabajo de Kushnirenko y Kharatishvili,[29] quienes están adscritos a la Universidad Estatal de San Petersburgo, Rusia, analiza el mecanismo de comisión de delitos cibernéticos, incluido el fraude, en torno a transacciones con criptomonedas. Desde el punto de vista de la criminalística y la ciencia forense, también observan la necesidad de un rápido desarrollo para responder a los constantes cambios producidos por las tecnologías y particularmente por los delitos de los que son objeto las transacciones con criptomonedas.

27 BISHT, Deepa *et al.,* "Imperative Role of Integrating Digitalization in the Firms Finance: A Technological Perspective", *Electronics (Switzerland)* 11, núm. 19, 2022, pp. 1-16, https://doi.org/10.3390/electronics11193252.

28 *Ibidem*, p. 4, traducción propia.

29 KUSHNIRENKO, Svetlana P. y KHARATISHVILI, Anton G., "Cryptocurrencies Turnover and Forensic Analysis of the Mechanism of Committing Crimes", *Kutafin Law Review* 9, núm. 4, 2022, pp. 774-792, https://doi.org/10.17803/2313-5395.2022.4.22.774-792.

Dada la revisión que llevan a cabo los autores, llegan a la conclusión de que "la criptodivisa puede actuar de dos formas a la hora de cometer delitos: directa e indirecta",[30] la primera es de mayor interés para este trabajo ya que incluye el acceso no autorizado a la *billetera* de las personas propietarias para cometerles fraude, sin embargo, ambas modalidades se describen a continuación.

Los autores consideran que, en su forma directa, la criptodivisa es objeto de delito cuando se tiene como finalidad la transferencia ilegal de derechos digitales del propietario al autor del delito o a otras personas, cometiendo, como se dijo, robo y/o fraude, incluso soborno. Mientras tanto, para su modalidad indirecta plantean que las transacciones son realizadas por su propietario, quien opera su *criptobilletera* sin signos de acceso no autorizado, por ejemplo, al transferir (pagar) dinero para la venta (adquisición) de drogas o como objeto de lavado de dinero, entre otras finalidades.[31]

En dicha investigación se hace énfasis en las grandes diferencias regulatorias en las legislaciones nacionales respecto de las criptomonedas o criptodivisas, incluida su prohibición o la ausencia de leyes al respecto. Con base en ello, da opciones basadas en evidencia científica para desarrollar herramientas que lleven a detectar e investigar eficazmente los delitos relacionados con criptomonedas (robo,[32] fraude, extorsión, lavado de dinero, corrupción, tráfico de drogas, entre otros) y su naturaleza electrónica, descentralizada, transfronteriza y supranacional, particularidades que, precisamente, han empleado los ciberdelincuentes para quedar impunes, es decir, para superar la fuerza de los Estados.

Una de las soluciones expuestas en el texto consiste en la formación de investigadores especializados de mano de expertos de todo el mundo, particularmente de los países con vasta experiencia en la materia. Otra muy particular en la rama penal del derecho, que atañe aún más al Poder Legislativo, es la de prever la incautación de criptomonedas cuando se requiera, incluso como medida cautelar, dotando la facultad a las instancias de investigación previa. Los autores señalan que tal

30 *Ibidem*, p. 779, traducción propia.

31 *Cfr*. *Idem.*

32 En este caso no se habla de robo de identidad toda vez que, dada la naturaleza de las criptodivisas y a decir del propio documento de Kushnirenko y Kharatishvili, la identificación del usuario que registra una *criptocartera* no requiere proporcionar ningún dato personal.

procedimiento ya "existe en Estados Unidos, donde los *criptoactivos* de las personas que por ley pueden ser objeto de incautación de sus bienes se transfieren a *criptocarteras* controladas durante medidas procesales y técnicas especiales, privando así a los sospechosos y acusados de los derechos de uso y disposición de criptodivisas".[33]

El trabajo de Choithani *et al.,*[34] se centra tanto en las criptomonedas como en el sistema bancario, así como en la utilidad de la Inteligencia Artificial como recurso para detectar y prevenir el fraude cibernético, con el impacto legal que esto representa.

Sus autores hacen énfasis en que los datos son hoy en día un activo de suma importancia para las empresas, los gobiernos y muchas otras organizaciones. Con ello también para los delincuentes y en particular para los ciberdelincuentes. De acuerdo con dicho trabajo, el incremento del comercio electrónico, así como del mercado de criptomonedas, se acompaña de que el fraude en línea también ha aumentado.

Con ello, "la seguridad de los datos está destinada a protegerlos del acceso no autorizado en todo su proceso de vida",[35] aspecto que, si bien se puede haber convertido en un freno del desarrollo tecnológico, a su vez es una de las principales razones de incorporar las bondades de los avances más recientes. En este contexto, la Inteligencia Artificial (junto con su aprendizaje automático), así como la ciberseguridad, también han avanzado con rapidez, lo que ha resultado de utilidad para la prevención del fraude cibernético y otros delitos en línea.

Los autores consideran que la Inteligencia Artificial representa una solución efectiva para ese propósito dado su comportamiento de trabajo que se asemeja e incluso mejora al del ser humano. Tan solo por poner un ejemplo, los autores traen a colación el mejoramiento del reconocimiento de voz e imagen en el proceso de identificación correcta de las personas usuarias del sistema bancario.

La investigación señala una serie de beneficios en la incorporación de técnicas derivadas de la Inteligencia Artificial en bancos e instituciones financieras, de entre las que destaca su capacidad de reconocer patrones

33 KUSHNIRENKO, Svetlana P. y KHARATISHVILI, Anton G., *op. cit.,* p. 787, traducción propia.

34 CHOITHANI, Tamanna *et al.,* "A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking System", *Annals of Data Science*, 2022, pp. 1-33, https://doi.org/10.1007/s40745-022-00433-5.

35 *Ibidem*, p. 3, traducción propia.

de datos sospechosos entre vastas cantidades de información para implementar la gestión del fraude y evitarlo, proporcionar avisos sobre ciberataques e identificar una variedad de problemas relacionados con las filtraciones de datos.

Derivado de dicha investigación, se puede decir que la Inteligencia Artificial es una realidad que debe contemplarse por parte de los actores políticos y las instancias legislativas, pues representa una herramienta en la detección y prevención de fraudes cibernéticos, necesaria para proteger a los usuarios y a las organizaciones.

El estudio cualitativo de Mambile y Mbogoro,[36] basado en una revisión bibliográfica, así como de entrevistas y encuestas, centra su atención en Tanzania y, específicamente, en la ciberseguridad y los ciberdelitos en el sector público de aquel país de África oriental, partiendo de que sus funcionarios, al hacer uso de la tecnología en el desempeño de sus tareas (lo que ha crecido considerablemente), desconocen diversos aspectos legales y técnicos del tema y de la inconsciente afectación que provocan a la ciudadanía.

Una interpretación que se hace a partir de dicha investigación es que la evidencia en aquel país demuestra que es necesario, primero, saber qué tanto conocen y desconocen sus funcionarios públicos en materia de regulación del uso de tecnología en el desempeño de sus obligaciones; y segundo, con base en ello, prever la obligación específica de capacitar y certificar al personal en materia de ciberseguridad y ciberdelitos. La principal finalidad de ello es cuidar los datos y en general la seguridad de los usuarios de servicios gubernamentales, así como de las personas contribuyentes. La sensibilización que esto produzca, además, evitará comprometer a las personas que trabajan en el gobierno en la posible comisión de delitos cibernéticos, incluso la protección de la institución para la que laboran.

La investigación concluye que, como Estado, es necesario mejorar en general las leyes cibernéticas, en el entendido de que sus funcionarios pueden delinquir consciente e inconscientemente sin ser castigados debido a que dichas conductas aún no están contempladas como delitos.

36 MAMBILE, Cesilia y MBOGORO, Peter E., "Cybercrimes awareness, cyber laws and its practice in public sector tanzania", *International Journal of Advanced Technology and Engineering Exploration* 7, núm. 68, 2020, pp. 119-126, https://doi.org/10.19101/IJATEE.2020.762051.

El documento de Barker,[37] por su parte, se centra en los usuarios de la banca electrónica, un área que es objeto de múltiples delitos cibernéticos tanto en Sudáfrica (país que estudia) como en México. La autora parte de la importancia de la concientización a las personas usuarias de servicios financieros en línea en cuanto a la prevención del fraude cibernético del que pueden ser objeto.

El trabajo describe la dificultad para detectar este tipo de delito, lo que hace indispensable la educación y la comunicación proactiva en cuanto a medidas antifraude principalmente con las personas usuarias que más desconocen del tema para reducir su vulnerabilidad, incluso, para mejorar su relación con los bancos.

En este sentido, las "medidas iniciadas por el gobierno para enfrentar los desafíos del sector bancario y cómo se intenta adaptar las medidas regulatorias de las mejores prácticas globales podrían ayudar al sector a volverse más sólido, eficiente y eficaz para prevenir las transacciones fraudulentas y mejorar la calidad de sus activos."[38] Las prevenciones que los bancos deben tener en cuenta, de acuerdo con la autora, deben ir acompañadas de actores gubernamentales, de tal forma que se asegure, a través de incentivos, por ejemplo, que exista esta medida preventiva del fraude cibernético.

En un estudio similar, acerca del fraude cibernético en el sector bancario, pero en el caso de India, el trabajo de Jeyanthi *et al.*,[39] afirma que la creación de medidas de protección contra los fraudes cibernéticos, así como la clara distinción en la ley de las estrategias a través de las cuales se pueden cometer, junto con la creación de medidas de control estrictas y el establecimiento de normas que coadyuven a la detección de la extorsión, no solo permiten a los bancos evitar la pérdida de recursos, sino que además mejoran la naturaleza de sus formas de negocio y su notoriedad general en el entorno empresarial.[40]

37 BARKER, Rachel, "The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention", *South African Journal of Business Management* 51, núm. 1, 2020, pp. 1-10, https://doi.org/10.4102/SAJBM.V51I1.1941.

38 NATARAJ, Geethanjali y ASHWANI, D., "Banking sector regulation in India: Overview, challenges and way forward", *Indian Journal of Public Administration*, 64(3), 2018, pp. 473-486 p. 484 citado por BARKER, Rachel, *op. cit.,* p. 9.

39 JEYANTHI, P. Mary *et al.,* "Significance of fraud analytics in Indian banking sectors", *Journal of Critical Reviews* 7, núm. 4, 2020, pp. 209-213, https://doi.org/10.31838/jcr.07.04.38.

40 *Cfr*. *Ibidem,* p. 209.

Los autores advierten que los bancos deben considerar, dentro de los constantes cambios en el sector originados por el fraude cibernético, la manera en que se verá afectado su modelo de negocio y su capacidad de respuesta debidos a las normas legales que intentan responder a ello. En esto, (al igual que Barker) incluyen la educación y comunicación con los clientes con la finalidad de ayudarles a reconocer y prevenir fraudes. En este sentido, se plantea una especie de asociación entre la industria bancaria, los usuarios de la banca en línea y el Gobierno para afrontar este problema.

Finalmente, el trabajo experimental de Fernandes y Antunes,[41] analiza la viabilidad del uso de herramientas forenses para extraer, analizar y reconstruir evidencias digitales en la persecución de múltiples delitos cibernéticos que hacen uso de la manipulación digital de imágenes y contenido multimedia, incluido el fraude financiero.

Si bien el estudio se centra en aspectos técnicos, se extrae que dichos recursos constituyen una verdadera ayuda para los persecutores del delito, particularmente para el personal que hace labores de investigación criminal, como la policía cibernética, toda vez que "la investigación que lleva a cabo un experto sin utilizar un conjunto de herramientas que le ayuden en tan ardua tarea ante millones de datos es una carga de tiempo poco factible";[42] su uso debe representar rapidez y precisión en los resultados.

De acuerdo con los autores, lo que ha permitido que el análisis forense digital con las características antes señaladas sea una realidad, es el uso de las herramientas técnicas adecuadas,[43] acompañado del surgimiento de procedimientos y normas legales que lo contemplan, (permiten u ordenan).

41 FERNANDES, Pedro y ANTUNES, Mário, "Benford's law applied to digital forensic analysis", *Forensic Science International: Digital Investigation,* 45, 2023, pp. 1-16, https://doi.org/10.1016/j.fsidi.2023.301515.

42 FERREIRA, Sara, "Photos-Videos-manipulations-dataset", *Github,* 2021, citado por FERNANDES, Pedro y ANTUNES, Mário, *op. cit.,* p. 2, traducción propia.

43 El texto se centra específicamente en el modelo basado en la denominada Ley Benford (no por su denotación jurídica) ante otros modelos basados en *Support Vector Machines* (SVM) y *Convolutional Neural Networks* (CNN), además, de hacer referencia a otras herramientas forenses como *Forensic Toolkit* (FTK), *Autopsy*, así como *ImageNet*.

IV. DISCUSIÓN: UTILIDAD EN EL ÁMBITO LEGISLATIVO MEXICANO

El marco jurídico vigente de nuestro país en materia de ciberseguridad y ciberdelincuencia se conforma por múltiples disposiciones constitucionales, legales y reglamentarias. Se trata de preceptos dentro de siete artículos de nuestra Constitución, de 29 normas secundarias y de 29 ordenamientos jurídico-administrativos federales.[44]

Específicamente en materia de robo de identidad y fraude cibernéticos a personas usuarias, la Ley para Regular las Instituciones de Tecnología Financiera, prevé en sus artículos 34, 39 y 58, de manera textual, lo siguiente:

> **Artículo 34.-** Las [Instituciones de Tecnología Financiera (ITF)] que operen con activos virtuales deberán **divulgar a sus Clientes**, además de lo previsto en esta Ley, **los riesgos que existen por celebrar operaciones con dichos activos**, lo que deberá incluir, como mínimo, informarles de manera sencilla y clara en su página de internet o medio que utilice para prestar su servicio, lo siguiente:
> **I.** El activo virtual no es moneda de curso legal y no está respaldado por el Gobierno Federal, ni por el Banco de México;
> **II.** La imposibilidad de revertir las operaciones una vez ejecutadas, en su caso;
> **III.** La volatilidad del valor del activo virtual, y
> **IV. Los riesgos** tecnológicos, cibernéticos y **de fraude inherentes a los activos virtuales**.
> **Artículo 39.-** Las solicitudes para obtener las autorizaciones de la [Comisión Nacional Bancaria y de Valores] previstas en el presente Capítulo deberán acompañarse de lo siguiente:
> […]
> **VI.** Las medidas y políticas en materia de control de riesgos operativos, así como de seguridad de la información, incluyendo

44 Véase "Normativa constitucional y legal sobre ciberseguridad vigente en México", así como "Ordenamientos jurídico-administrativos federales sobre ciberseguridad" en MARÍN HERNÁNDEZ, Gustavo Eduardo y GÓMEZ LARA, Irving Ilie, *La ciberseguridad: Un estudio comparado,* Centro de Estudios de Derecho e Investigaciones Parlamentarias, Cámara de Diputados, 2022, pp. 107-124. Cabe señalar que los autores advierten en su publicación que se trata de listados no exhaustivos.

> las políticas de confidencialidad, con la evidencia de que cuentan con un soporte tecnológico seguro, confiable y preciso para sus Clientes y con los estándares mínimos de seguridad que aseguren la confidencialidad, disponibilidad e integridad de la información y **prevención de fraudes** y ataques cibernéticos, de conformidad con lo establecido en las disposiciones de carácter general aplicables;
> […]
> **IX.** Las políticas de **prevención de fraudes** y prevención de operaciones con recursos de procedencia ilícita y financiamiento al terrorismo;
> […]
> **Artículo 58.-** […]
> […] la Secretaría, considerando las características de las Operaciones y actividades llevadas a cabo por las ITF, en las disposiciones de carácter general a que se refiere este artículo, emitirá los lineamientos sobre el procedimiento y criterios, así como los casos, la forma, los términos y los plazos en que las ITF deberán observar respecto de:
> […]
> **II.** La información y documentación que las ITF deban recabar para la celebración de las Operaciones y servicios que presten y que acredite plenamente la **identidad** de sus Clientes;
> […] [énfasis añadido]

Como se lee, dicha ley contiene ciertos mandatos que atienden, aunque solo a nivel preventivo, los delitos en comento. También en este orden de ideas vale la pena aludir la reforma del 16 de abril de 2021 a la Ley Federal de Telecomunicaciones y Radiodifusión, la cual hacía mención expresa a la prevención del robo de identidad a usuarios, derivado de la venta, cesión, hurto o extravío de sus equipos o tarjetas *SIM*,[45] a través de campañas informativas por parte de autoridades y concesionarios, las que incentivaran la obligación de denunciarlo o reportarlo en forma inmediata.

45 Acrónimo de *Subscriber Identity Module,* la tarjeta SIM es empleada en equipos móviles de comunicación para almacenar información e identificar al usuario.

Si bien se podría estar ante una modalidad de robo de identidad originada de manera física mediante otro delito, este forma parte de las sugerencias de las personas estudiosas del tema, concretamente en cuanto a la prevención de los delitos mediante el involucramiento de diversos actores, de llevar a cabo acciones divulgativas, así como de diferenciar en la ley entre los comportamientos delictivos *físicos* (fuera de línea) y cibernéticos (en línea), junto con la posibilidad de transición entre un ambiente y otro.

No obstante, este precepto normativo, siendo parte de una modificación legislativa más amplia (acerca del Padrón Nacional de Usuarios de Telefonía Móvil), fue declarado inválido por sentencia de la Suprema Corte de Justicia de la Nación que resolvió la Acción de Inconstitucionalidad 82/2021,[46] notificada para efectos legales un año más tarde al de su publicación, quedando sin vigencia desde abril de 2022.

Además de estos dispositivos, entre los vigentes y este último que fue expulsado del orden jurídico nacional, existen otros que hacen referencia al robo de identidad y fraude, sin embargo, lo hacen en referencia a una afectación a instituciones y a su personal (como en la Ley de Instituciones de Crédito) o de manera física (en diversos ordenamientos, como en el Código Penal Federal).

Los actos delictivos de robo de identidad y fraude cometidos en un ambiente cibernético en contra de usuarios carecen de una regulación integral, clara, precisa y actualizada. Otras investigaciones desde el ámbito legislativo observan que incluso abarca una ausencia de tipificación en la legislación penal mexicana,[47] a pesar de ser estos delitos de los pendientes en materia de ciberseguridad que más afectan y afectarán a las y los mexicanos,[48] ya que esto trae como resultado su impunidad y, por consiguiente, que su incidencia incremente al pasar del tiempo.

46 Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021 promovida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y diversos Senadores integrantes de la LXIV Legislatura, contra el Congreso de la Unión y otra autoridad, demandando la invalidez del Decreto por el cual se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión, publicado en el Diario Oficial de la Federación el 16 de abril de 2021.

47 *Cfr.* MARÍN HERNÁNDEZ, Gustavo Eduardo y GÓMEZ LARA, Irving Ilie, *op. cit.,* pp. XIX, XX, 8 y 12.

48 AGUIRRE QUEZADA, Juan Pablo, "Ciberseguridad, desafío para México y trabajo legislativo", Cuaderno de investigación, núm. 87, Senado de la República, Instituto Belisario Domínguez, marzo 2022, pp. 9 y 20.

Además, en términos generales, a pesar de que el marco jurídico federal contempla algunos aspectos relacionados con la ciberseguridad de las personas usuarias, cabe señalar que México aún no cuenta con una ley específica en la materia, que se encuentre vigente y que lleve a cabo una regulación a la altura del fenómeno, es decir, que responda las necesidades para su combate en concordancia con su naturaleza, tal como se recomienda en los instrumentos internacionales y en las investigaciones que se revisan dentro de este trabajo.

Con todo, existen múltiples esfuerzos en el Poder Legislativo que proponen la expedición de una ley sobre ciberseguridad, así como cambios en la materia dentro de la Constitución Política de los Estados Unidos Mexicanos y de normas secundarias como la Ley de Seguridad Nacional, la Ley General del Sistema Nacional de Seguridad Pública, la Ley de Seguridad Nacional, la Ley de la Fiscalía General de la República, el Código Penal Federal, entre otras.[49]

En este contexto, los hallazgos de este trabajo se enlistan a continuación a manera de aspectos que, de acuerdo con los autores analizados, deberían ser contemplados en cualquier marco regulatorio en materia de ciberseguridad y ciberdelincuencia, específicamente en cuanto al robo de identidad y fraude cibernéticos. En la Tabla 3, dichos elementos se desglosan y describen por subtema, partiendo de que todos buscan reducir la comisión de los ciberdelitos mediante una legislación que permita su identificación, persecución y castigo para así evitar su impunidad y proteger a las personas usuarias en su identidad, patrimonio e integridad.

49 Véase "Trabajo legislativo en el tema de ciberseguridad" en AGUIRRE QUEZADA, Juan Pablo, *op. cit.,* pp. 10-15; así como "Iniciativas sobre ciberseguridad" en MARÍN HERNÁNDEZ, Gustavo Eduardo y GÓMEZ LARA, Irving Ilie, *op. cit.,* pp. 8-11.

Tabla 3. Aspectos aconsejados en la literatura para ser contemplados en el marco jurídico sobre robo de identidad y fraude cibernéticos, así como su utilidad.

PRECEPTO / ELEMENTO	UTILIDAD ESPECÍFICA	FUENTE(S)
1. Insumos para el desarrollo de legislación en la materia y aspectos generales		
Marco Convencional: Convenio de Budapest	Guía básica para el desarrollo de legislación para combatir el ciberdelito; proporciona una solución integral, operativa y funcional para la investigación y el enjuiciamiento del delito cibernético.	Mayer Lux y Oliver Calderón; Khan *et al.*
Tratados internacionales y leyes modelo	Armonización legislativa con leyes de países a la vanguardia; cooperación internacional; política criminal común entre países para disuadir a los ciberdelincuentes de manera efectiva mediante la coordinación, de tal manera que se facilite la detección del ciberdelito, la recopilación de pruebas, la investigación y, finalmente, el enjuiciamiento.	Khan *et al.*
Legislación especializada y actualizada	Tipificar el delito cibernético y otorgar facultades procesales suficientes para investigar.	Khan *et al.*
Delimitación clara de los delitos	Diferenciación entre conductas delictivas similares y su correcta tipificación; evitar tipificación genérica de "delitos cibernéticos"; especificación puntual de sus características.	Mayer Lux y Oliver Calderón; Jeyanthi *et al.*
Especificar atribuciones, derechos y obligaciones de actores clave: autoridades y personas usuarias, proveedores de internet, etc.	Contar con cooperadores en la detección, prevención y respuesta a los delitos cibernéticos; asegurar derechos de las personas usuarias.	Khan *et al.;* Guo *et al.*
Prever el incremento de la gravedad y frecuencia de los engaños cibernéticos, así como su conducción a delitos fuera de la red	Diferenciar comportamientos fraudulentos en línea y fuera de línea y, a la par, la transición del delito; se evita que el proceso penal quede inconexo.	Guo *et al.*
Obligatoriedad de mensajes y campañas por parte de instancias gubernamentales y de proveedores de servicios financieros en línea	Concientización a las personas usuarias, principalmente las más vulnerables para ayudarles a reconocer y prevenir fraudes (prevención y educación proactiva reduciendo la brecha digital).	Khan *et al.*; Barker; Jeyanthi *et al.*
2. Uso de herramientas forenses y otras de avanzada		
Formación y capacitación constante, así como equipamiento, ambos con base en los últimos avances tecnológicos	Contar con investigadores especializados, efectividad en su labor.	Khan *et al.*; Kushnirenko y Kharatishvili
Uso de herramientas forenses avanzadas especificas por parte de la policía cibernética	Extraer, analizar y reconstruir evidencias digitales en la persecución de delitos cibernéticos con rapidez y precisión en los resultados.	Fernandes y Antunes
Previsión y permisión del uso de herramientas técnicas en la investigación de delitos, tales como *honeypots.*	Permitir el uso de herramientas a persecutores del delito; obtener información valiosa de las personas atacantes y sus métodos; efectividad en la persecución del delito.	Guo *et al.*

Incorporación en la banca de las distintas tecnologías de la Industria 4.0 como internet de las cosas, *big data*, la automatización de procesos robóticos y el *blockchain.*	Mejorar la calidad, accesibilidad y, principalmente, la seguridad de sus productos y servicios, principalmente en línea. (Asegurando la interoperabilidad, así como la disponibilidad del espectro).	Bisht *et al*.
Capacitación y certificación de todo servidor público que haga uso de tecnología	Cuidar los datos y en general la seguridad de los usuarios de servicios gubernamentales, incluidas las personas contribuyentes, los propios servidores públicos, así como las instituciones.	Mambile y Mbogoro
3. Criptodivisas e Inteligencia Artificial		
Diferenciación de dos formas principales de comisión de delitos con criptomonedas: directa (transferencia ilegal de derechos: robo, fraude o soborno) e indirecta (lavado de dinero, compra de narcóticos)	Correcta regulación de criptomonedas en legislaciones nacionales; prever sus particularidades (naturaleza electrónica, descentralizada, transfronteriza y supranacional).	Kushnirenko y Kharatishvili
Prever la incautación de criptomonedas cuando se requiera, incluso como medida cautelar, dotando la facultad a las instancias de investigación previa	Posibilidad de transferir *criptoactivos* a carteras controladas durante medidas procesales y técnicas; privar a los sospechosos y acusados de los derechos de uso y disposición de criptodivisas.	Kushnirenko y Kharatishvili
Uso de Inteligencia Artificial y aprendizaje automático (como en el reconocimiento de voz e imagen en la identificación de personas usuarias del sistema bancario)	Comportamiento semejante y mejorado del ser humano en tareas de combate al ciberdelito; reconocer patrones de datos sospechosos entre vastas cantidades de información; proporcionar avisos sobre ciberataques; identificar problemas relacionados con las filtraciones de datos.	Choithani *et al.*

Fuente: Elaboración propia a partir de los textos analizados.

V. CONCLUSIONES

La RSL es una metodología ampliamente utilizada en la investigación científica para sintetizar y sistematizar la evidencia sobre un tema específico. Su objetivo es identificar, seleccionar y evaluar críticamente estudios relevantes y proporcionar una síntesis objetiva de los resultados. La RSL facilita el avance del conocimiento, ayuda a desarrollar teorías, proporciona evidencia de alto nivel para la toma de decisiones y examina la bibliografía publicada en un contexto específico.

Aunque la RSL ofrece múltiples beneficios, se utiliza poco en los estudios legislativos debido al tiempo que requiere. Sin embargo, en este trabajo se propuso una adaptación de la metodología para que sea más eficiente y útil en el ámbito legislativo. En particular, se lleva a cabo una meta-revisión de la literatura mediante la selección de

publicaciones que ya han revisado fuentes primarias elaboradas bajo diversas metodologías y enfoques.

Las preguntas de investigación que guiaron este trabajo se centraron en los hallazgos de la literatura científica sobre medidas legales efectivas para combatir la ciberdelincuencia, específicamente el robo de identidad y el fraude. Además, se examinaron los preceptos normativos sugeridos en la literatura y se identificaron aquellos considerados relevantes con base en la evidencia existente.

Dentro de los hallazgos, se enfatiza la importancia de tipificar el fraude cibernético como un delito con tres características definitorias: manipulación de datos o programas, causar perjuicio patrimonial ajeno y presencia de ánimo de lucro. Requisitos que deben cumplirse simultáneamente para poder afirmar que se trata de fraude cibernético y evitar la impunidad.

Por otro lado, se destacó la debilidad de la legislación y campañas de sensibilización y prevención insuficientes como factores que contribuyen al aumento de los delitos cibernéticos en el mundo. Como una manera de enfrentar el problema, se resaltó la utilidad del Convenio de Budapest como un instrumento que proporciona una solución integral y funcional para investigar y enjuiciar delitos cibernéticos a nivel nacional e internacional. También se dio cuenta de otros tratados y acuerdos internacionales, así como de leyes modelo, a manera de insumos para desarrollar legislación nacional en la materia, que esté alineada con los estándares internacionales.

Asimismo, se destacó la preocupación por las implicaciones legales y éticas de la investigación policial en este ámbito, en el entendido que puede violar la privacidad de los usuarios y otros de sus derechos. Con lo que se concluye que se necesitan directrices y normas más específicas y claras para los investigadores, que les permitan realizar su trabajo dentro de un marco legal adecuado.

Además, la literatura subraya la necesidad de normas que consideren el aumento de la gravedad y frecuencia de los engaños cibernéticos, así como la transición entre delitos en línea y fuera de línea, distinción que la legislación debe contemplar.

Por otro lado, los estudios sobre el fraude cibernético en el sector financiero y las criptomonedas resaltan la importancia de incorporar tecnologías avanzadas, como el internet de las cosas, el *big data*, la

automatización de procesos robóticos y el *blockchain*, para detectar y prevenir este tipo de delitos. Se identifican problemas legales y regulatorios que deben abordarse para mejorar la calidad, accesibilidad y seguridad de los productos y servicios financieros.

De igual forma, se destacó el papel de la Inteligencia Artificial en la identificación de patrones sospechosos, la prevención de ciberataques y la protección de datos en el ámbito de las criptomonedas y el sistema bancario. También se resaltó la importancia de la concientización de los usuarios de la banca electrónica, la educación y la comunicación proactiva para reducir la vulnerabilidad frente al fraude cibernético.

Es necesario fortalecer las medidas de protección, establecer claras distinciones legales y aplicar normas estrictas para prevenir los fraudes cibernéticos en el sector bancario. Esto implica considerar el impacto en el modelo de negocio de los bancos, mejorar las leyes cibernéticas y fomentar la colaboración entre la industria bancaria, los usuarios y el Gobierno.

En lo que respecta al sector público, la capacitación y certificación en ciberseguridad del personal y la mejora de las leyes cibernéticas son fundamentales para proteger los datos y la seguridad de los usuarios de servicios gubernamentales y combatir la impunidad.

Finalmente, en términos de investigación forense, se destaca la importancia de utilizar las herramientas técnicas adecuadas, cumplir con los procedimientos y normas legales, así como trabajar en colaboración para lograr resultados rápidos y precisos en la persecución de delitos cibernéticos.

El marco jurídico mexicano vigente en materia de ciberseguridad y ciberdelincuencia muestra la falta de una ley específica que la regule y una ausencia de tipificación en la legislación penal para abordar el robo de identidad y el fraude cibernéticos. Esto ha generado un aumento significativo en la incidencia de estos delitos y una falta de protección para los usuarios. A pesar de ello, se han realizado importantes esfuerzos desde el Poder Legislativo para proponer una ley sobre ciberseguridad y realizar cambios en diversas normas.

Los aspectos identificados en este trabajo mediante la meta-revisión sistemática de la literatura, de acuerdo con sus autores, deberían ser considerados en cualquier marco regulatorio en materia de ciberseguridad y ciberdelincuencia, con el objetivo de reducir la

comisión de ciberdelitos, identificarlos, perseguirlos y castigarlos para evitar la impunidad y proteger a los usuarios en su identidad, patrimonio e integridad.

Asimismo, derivado de los estudios que se analizaron, se puede resaltar la necesidad de una aproximación multidisciplinaria, donde converjan la tecnología, la regulación, la educación y la cooperación entre diferentes actores para hacer frente al fraude cibernético y proteger los sistemas financieros y los datos de los usuarios.

Para combatir eficazmente los delitos cibernéticos y reducir su incidencia sustantivamente, es de suma importancia contar con una legislación clara, precisa y actualizada; es fundamental tipificarlos y delimitarlos adecuadamente, así como adoptar los beneficios de la cooperación entre naciones y la adopción de preceptos provenientes de instrumentos jurídicos internacionales, en favor de los trabajos legislativos en México.

VI. REFERENCIAS

1. *Bibliohemerográficas*

AGUIRRE QUEZADA, Juan Pablo, "Ciberseguridad, desafío para México y trabajo legislativo", *Cuaderno de investigación*, núm. 87, Senado de la República, Instituto Belisario Domínguez, marzo 2022.

BARKER, Rachel, "The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention", *South African Journal of Business Management* 51, núm. 1, 2020.

BISHT, Deepa, SINGH Rajesh, GEHLOT Anita, VASEEM AKRAM Shaik, SINGH Aman, CARO MONTERO Elisabeth, PRIYADARSHI Neeraj y TWALA Bhekisipho, "Imperative Role of Integrating Digitalization in the Firms Finance: A Technological Perspective", *Electronics (Switzerland)* 11, núm. 19, 2022.

CASSIM, Fawzia, "Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?", *Potchefstroom Electronic Law Journal* 18, núm. 2, 2015.

CHANG, Lennon, "Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia", en HOLT, Thomas y BOSSLER,

Adam (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Palgrave Macmillan, Cham, 2020.

CHOITHANI, Tamanna, CHOWDHURY, Asmita, PATEL, Shriya, PATEL, Poojan, PATEL, Daxal, SHAH, Manan, "A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking System", *Annals of Data Science*, 2022.

FERNANDES, Pedro y ANTUNES, Mário, "Benford's law applied to digital forensic analysis", *Forensic Science International: Digital Investigation*, 45, 2023.

FETTKE, Peter, "State of the Art des State of the Art Wirtschaft", *Informatik*, 48-257, 2006.

GUO, Zhen CHO, Jin-Hee, CHEN, Ing-Ray, SENGUPTA, Srijan, HONG, Michin y MITRA, Tanushree, "Online Social Deception and Its Countermeasures: A Survey", *IEEE Access* 9, 2021.

ICART ISERN, María Teresa y CANELA SOLER, Jaume, "El artículo de revisión", *Enferm Clin*, 4(4), 1994.

JEYANTHI, P. Mary, MANSURALI, Anifa, HARISH, Venkatasubramanian y KRISHNAVENI, Damodaran, "Significance of fraud analytics in Indian banking sectors", *Journal of Critical Reviews* 7, núm. 4, 2020.

KHAN, Shereen, SALEH, Tajneen, DORASAMY, Magiswary, KHAN, Nasreen, TAN SWEE LENG, Olivia, GALE VERGARA Rossanne, "A systematic literature review on cybercrime legislation", *F1000 Research* 11, núm. 971, 2022.

KUSHNIRENKO, Svetlana P. y KHARATISHVILI, Anton G., "Cryptocurrencies Turnover and Forensic Analysis of the Mechanism of Committing Crimes", *Kutafin Law Review* 9, núm. 4, 2022.

MAMBILE, Cesilia y MBOGORO, Peter E., "Cybercrimes awareness, cyber laws and its practice in public sector tanzania", *International Journal of Advanced Technology and Engineering Exploration* 7, núm. 68, 2020.

MARÍN HERNÁNDEZ, Gustavo Eduardo y GÓMEZ LARA, Irving Ilie, *La ciberseguridad: Un estudio comparado*, Centro de Estudios de Derecho e Investigaciones Parlamentarias, Cámara de Diputados, 2022.

MAYER LUX, Laura y OLIVER CALDERÓN, Guillermo, "El delito de fraude informático: concepto y delimitación", *Revista Chilena de Derecho y Tecnología* 9, núm. 1, 2020.

NATARAJ, Geethanjali y ASHWANI, D., "Banking sector regulation in India: Overview, challenges and way forward", *Indian Journal of Public Administration*, 64(3), 2018.

RAMOS, Miguel H., RAMOS, Mara Florencia y ROMERO Enrique, "Cómo escribir un artículo de revisión", *Revista de postgrado de la VI Catedra de Medicina*, 2003.

SKIAS, Dimitrios, TSEKERIDOU, Sofia, ZAHARIADIS, Theodore, VOULKIDIS, Artemis, VELIVASSAKI, Terpsichori-Helen, "Demonstration of alignment of the pan-european cybersecurity incidents information sharing platform to cybersecurity policy, regulatory and legislative advancements", en *ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security*, Nueva York, Association for Computing Machinery, 2022.

WEBSTER, Jane y WATSON, Richard T., "Analyzing the Past to Prepare for the Future Writing a Literature Review", *MIS Quarterly*, 26-2, 2002.

2. *Internet*

ELSEVIER, *Scopus. Guía rápida de referencia*.

3. *Otros*

FERREIRA, Sara, "Photos-Videos-manipulations-dataset", *Github,* 2021.