https://doi.org/10.18800/dys.202501.014

FECHA DE RECEPCIÓN: 06/03/2025
FECHA DE APROBACIÓN: 15/05/2025

Andar y desandar sobre la victimología del cibercrimen (dos décadas después)

Back and forth on the victimology of cybercrime (two decades later)

Luis Miguel Reyna Alfaro*
Caro & Asociados

Resumen:
El cibercrimen es un fenómeno delictivo particularmente complejo y frente al que el sistema penal revela sus mayores retos y dificultades. Uno de ellos se vincula con la víctima del delito, actor central de la dinámica del delito, y cuyo dimensionamiento resulta trascendente para la configuración de los diseños de política criminal. El presente estudio proporciona una aproximación inicial para el desarrollo de la victimología del cibercrimen en tanto herramienta central del conocimiento criminológico que debe servir de pauta de orientación de las respuestas legislativas contra el cibercrimen.

Palabras clave:
Cibercrimen — delitos informáticos – víctima – victimología — cifra oculta de criminalidad — estadística criminal.

Abstract:
Cybercrime is a particularly complex criminal phenomenon, and one in which the criminal justice system faces its greatest challenges and difficulties. One of these concerns the victim of crime, a central actor in the dynamics of crime, whose dimension is crucial for shaping criminal policy designs. This study provides an initial approach to the development of cybercrime victimology as a central tool of criminological knowledge that should serve as a guideline for legislative responses to cybercrime.

Keywords:
Cybercrime — computer crimes — victim — victimology — hidden crime figures — criminal statistics.

* Abogado. Socio de Caro & Asociados. Maestro en Derecho Procesal por la Pontificia Universidad Católica del Perú (Perú). Maestro en Educación Superior e Investigación por INEJ (Nicaragua). Doctorando en Derecho Penal en la Universidad de Granada (España). Vicepresidente del Grupo Peruano de la Asociación Internacional de Derecho Penal.

1. Puntos de partida

Hace más de dos décadas (Reyna, 2002), en una de mis primeras monografías, destacaba cómo la irrupción de nuevas tecnologías había significado la transformación de una serie de instituciones jurídicas, y reconocíamos la necesidad de adaptarlas a esa nueva realidad virtual que llamamos *ciberespacio.*

Dentro de los escenarios de adaptación y transformación que pueden identificarse, uno de los de mayor interés es el correspondiente a la categoría conocida como *cibercrimen,* que ha emergido como un tópico de especial preocupación, no solo desde la perspectiva de teorización técnico dogmática, sino también desde el análisis criminológico.

Son, probablemente, dos las razones principales de la actual atención al cibercrimen: por un lado, por su cada vez más notoria relación con el crimen organizado —que abordamos con mayor detenimiento en anterior oportunidad (Reyna, 2016)—; y, en segundo término —aunque vinculado al anterior tópico— por su especial magnitud y dimensión lesiva. Dos décadas después, dedicaremos las líneas que siguen a identificar el *estado del arte* de la victimología del cibercrimen recurriendo a una narrativa en el que los *flashbacks* serán una suerte de constante.

2. La desmarginalización de la víctima en el Derecho penal

El Derecho Penal ha enfocado su atención, tradicional y mayoritariamente, hacia el/la agente activo(a) de la infracción penal: el/la victimario(a). Esta situación ha llevado a Hassemer a afirmar que el moderno Derecho Penal se inicia "con la neutralización de la víctima" (Reyna Alfaro, 2006, p. 109), fenómeno que, como deja de manifiesto Albin Eser (1998), encontró su punto "álgido" durante el debate de reforma penal alemán de los setenta del siglo XX, especialmente en las discusiones del proyecto Alternativo Alemán en las que el principio de "resocialización del delincuente" fue dotado de la misma jerarquía que el principio de protección de bienes jurídicos como uno de los fines de la pena (Roxin, 1982) y que tuvo importante influencia en las reformas penales de nuestra región a partir de la década de los ochentas del siglo pasado.

Sin embargo, particularmente en las últimos cuarenta años, la ciencia del Derecho Penal ha vuelto su mirada hacía la víctima, en un proceso que ha cobrado notoriedad a tal magnitud que no se hace sino hablar del "redescubrimiento", "renacimiento" de la víctima o, en el ámbito procesal, de "devolución" del conflicto a la víctima (Reyna Alfaro, 2006).

Este fenómeno de —para ser más exactos— *desmarginalización de la víctima del delito* es parte de un *corsi e ricorsi* que transita desde la *edad de oro* de la víctima del delito (derecho romano primitivo, el derecho germánico y el derecho medieval) y que se caracterizó por que la reacción punitiva quedaba a cargo de la víctima o sus cercanos (venganza privada), hasta la *monopolización del ius puniendi* por parte del Estado en el que la víctima carece de intervención en la relación punitiva (que se produce entre el victimario y el Estado) y se limita su posición a la relación indemnizatoria que tendría con el victimario y que se regula por el derecho civil (Silva Sánchez, 1993) y que encuentra, en lo que sería un *ricorsi,* el actual estadio de *redescubrimiento de la víctima del delito* y del reconocimiento del *principio de protección de la víctima del delito* (Villavicencio, 2000) como manifestación particular del Estado Social y Democrático de Derecho al ser una expresión de la tutela a las poblaciones vulnerables.

Pero no son solo razones de índole altruista y de cumplimiento de premisas constitucionales las que justifican la especial atención actual a la víctima del delito, sino razones de eficacia. El abordaje del fenómeno criminal —como ha sabido referir el maestro mexicano Rodríguez Manzanera— no puede explicarse sin el análisis de la víctima del delito (1995). Sin esa perspectiva cualquier reflexión sobre la cuestión criminal será siempre parcial y, por ende, imprecisa.

3. La criminalidad informática como manifestación de la "sociedad del riesgo"

Las sociedades modernas se encuentran configuradas como verdaderas *sociedades del riesgo* (Beck, 2006), en las cuales los efectos adversos del desarrollo de la tecnología, la producción y el consumo adquieren nuevas dimensiones y provocan riesgos masivos a los ciudadanos, los ejemplos más característicos los ubicamos en el tráfico vehicular, la comercialización de productos peligrosos o la contaminación ambiental (Reyna Alfaro: 2002a; Reyna Alfaro, 2016).

En este contexto, las tecnologías de la información y la comunicación (TIC's) —sin soslayar su importancia en la evolución científica y en la dinámica social— poseen también matices negativos (riesgos) que son de interés del derecho penal y de la criminología. No es de extrañar que se reconozca al derecho penal informático como una "faceta" de los riesgos virtuales (Elbert, 2007; Faraldo, 2009).

La criminalización de los cibercrímenes aparece así dentro del proceso de *expansión del derecho penal* que ha descrito magistralmente Jesús María Silva Sánchez (2001), caracterizado por la inflación del ordenamiento jurídico penal (un derecho penal más amplio y más severo). Esta aseveración será objeto de corroboración a través de las particularidades propias de la víctima del cibercrimen.

4. La importancia del estudio de la víctima del delito para el conocimiento del cibercrimen

Ya lo indicaba von Hentig, uno de los padres de la victimología: "En el derecho penal al autor le corresponde siempre una víctima" (1972, p. 408). No será este el lugar para resaltar la importancia del estudio de la víctima para comprender las auténticas dimensiones del fenómeno criminal y, especialmente, para reconocer el modo en que los ofensores implementan sus estrategias y manipulaciones informáticas para concretar los cibercrímenes (Durán Valladares, 2002).

En efecto, ya indicaba von Hentig que la víctima no es un objeto inanimado sino un elemento activo en la dinámica del delito (1962). Este rol —como correctamente puso en evidencia el maestro peruano Alejandro Solís Espinoza— ya había sido resaltado en 1939 por Franz Exner (1988). Precisamente por este motivo es que se resalta la trascendencia del estudio de la víctima del delito para los efectos de prevenir la criminalidad, particularmente en el contexto de la sociedad de riesgo (Neuman, 1984).

En lo que sigue procuraremos incorporar algunos postulados iniciales que —a modo de anclaje— permitan una aproximación coherente a la figura de la víctima del cibercrimen.

5. Orientaciones iniciales hacia la victimización en el cibercrimen.

5.1. Aproximaciones iniciales y su orientación al predominio de la persona jurídica como víctima del cibercrimen

Desde los análisis iniciales, en los que las tecnologías de la información virtual no se habían aún masificado y se confinaba a ciertos planos específicos de la vida (como el ámbito financiero), hasta el presente, las visiones sobre la víctima de estos delitos han ido evolucionando y esto ha ocurrido de la mano con el desarrollado conceptual del *cibercrimen*.

En efecto, mientras la conceptualización inicial en la materia parecía vincularse más a los elementos físicos (*hardware*) o inmateriales (*software*) de la informática, lo que permite reconocer ciertas correlaciones entre los conceptos de *computer crime*, de uso en el derecho anglosajón, y los *delitos informáticos,* predominante en la doctrina propia del *civil law*, el estado actual de cosas parece aceptar la necesaria vinculación conceptual del delito con el uso de las tecnologías de la información y el uso del internet. Esta transición ha provocado que la visión tradicional de la víctima del *computer crime* se haya trasladado desde las personas jurídicas y las organizaciones empresariales hacia los individuos.

Esta visión inicial, resaltada en los planteos de Gutiérrez (1991), Magliona y López (1999), Bramont Arias (1997) o Alarcón (2019), identifica a la persona jurídica como *la víctima por excelencia del delito informático* (Gutiérrez, 1991). Este dato, por cierto, venía incentivado por el surgimiento de un movimiento que veía el *hacking* como una herramienta ética para hacer frente a las excesos de las corporaciones empresariales.

La vinculación de la víctima del delito informático con la persona jurídica tiene una serie de consecuencias destacadas por la doctrina: (i) la victimización suponía para la persona jurídica un significativo daño reputacional y patrimonial pues revela la ineficacia de las medidas de protección informática establecidas por aquella y la vulnerabilidad de sus sistemas de seguridad informática; y, (ii) la condición anterior provocaba un escaso interés de la víctima del delito por poner en conocimiento de las autoridades el hecho cometido en su agravio (Alarcón, 2019; Faraldo, 2009; Gutiérrez, 1991; Jiménez, 2017). En un escenario como el antes descrito, la persona jurídica victimada se expone a ser considerada una *víctima colaboradora* (Gutiérrez, 1991) y, con ello, no solo asumir el riesgo de propiciar la impunidad del victimario —por autopuesta en riesgo (Bramont Arias, 1997)— sino que podría provocar efectos de victimización adicionales (efectos derivados de los cuestionamiento que se generarían sobre su seguridad informática, entendida como un factor de competitividad especialmente trascendente).

Aunque la victimización causada por el cibercrimen sobre las personas jurídicas y organizaciones sigue siendo un tópico de interés permanente (Alarcón, 2019; Grabosky, 2015), la utilización de redes sociales y la mayor conectividad informática parece revelar un incremento en la exposición al riesgo de cibercrimen de las personas naturales (Escobar *et al*., 2019; Grabosky, 2015) lo que ha llevado a algunos autores —como Miró Llinares (2015)— a proponer que la adopción del término cibercrimen se relaciona más con el predominio de las relaciones interpersonales en redes.

El nivel de exposición al cibercrimen de las personas naturales se incrementa en un escenario como el actual en el que la información personal fluye tanto en el contexto de las relaciones con la administración estatal como las organizaciones privadas particularmente en el plano de las relaciones de consumo (Valls, 2017). De allí la trascendental relación de la prevención del cibercrimen con la protección óptima de los datos personales.

6. Los perfiles y las tipologías de víctima del delito

La determinación de los patrones o caracteres que identifican a las víctimas del cibercrimen han sido siempre cuestión de difícil resolución o consenso. Menos aún parece posible proponer una particular tipología de la ciber-víctima (Miró Llinares, 2013), circunstancia que —por cierto— parece ser una di-

ficultad general de la victimología que ha pretendido —sin niveles de consenso plausibles en mi opinión— reconocer diversas tipologías de víctima del delito[1].

Pese a esta dificultad, el trabajo científico dentro de la victimología no puede renunciar a la pretensión de reconocer tipologías particulares de víctimas, allí donde aquello fuera posible, pues constituyen un factor relevante y útil para la sistematización de la información científica que se obtenga (Herrera, 2006).

En ese contexto, una de las propuestas de sistematización de los enfoques clasificatorios de la víctima del delito que resulta más atractivas es aquella que proviene de Herrera (2006) y que parte de dos ejes tipológicos: (i) la contribución de la víctima del delito; y, (ii) la vulnerabilidad de la víctima, que resultan criterios que se relacionan y complementan dependiendo de las circunstancias particulares. Precisamente serán esos los criterios que utilizaremos en lo que sigue de nuestro desarrollo.

7. La capacidad de rendimiento de la contribución y la vulnerabilidad de la víctima como enfoque de clasificación de la víctima del cibercrimen.

7.1. La contribución de la víctima en el cibercrimen

El análisis y valoración del modo en que el comportamiento de la víctima influye en la dinámica del delito ha sido de particular interés de la dogmática penal y la victimología desde siempre. Por ello, autores como von Hentig (1972) resaltan cómo es que ciertos tipos penales se construyen otorgando a la reacción de la víctima un rol relevante en el delito.

a) Asunción de riesgos: anonimato de los contactos en el ciberespacio.

El libre desarrollo de la personalidad solo puede ser comprendido si dentro de aquél se proyecta —como parte de su contenido— la libertad informática. El ejercicio de esa libertad por parte del ciudadano puede desarrollarse en contextos de riesgos que la persona asume voluntariamente.

Uno de esos riesgos es el del anonimato del espacio virtual: la interacción con personajes cuya identidad no se encuentra verificada puede incrementar significativamente el riesgo propio de los contactos sociales. Precisamente el anonimato de la interacción virtual es uno de los factores que contribuyen a crear las condiciones que propician situaciones de cibercriminalidad (Barrio, 2017). Las razones de esta afirmación se formulan seguidamente.

En primer lugar, el anonimato en internet es el que incentiva la proliferación de mercados ilícitos que se desarrollan en el entorno virtual y cuyos aspectos financieros son de difícil trazabilidad debido al uso de *criptoactivos* (Holt *et al.*, 2016) e ingenierías financieras sumamente complejas que invisibilizan al beneficiario final.

Por otro lado, el anonimato en internet y redes sociales parecen incentivar ciertas expresiones de la cibercriminalidad como el *cyberbulling* (similar, Miró Llinares, 2013), que son a su vez incentivadas por un marco legal poco consciente de la dañosidad de este tipo de conductas, especialmente en el caso de víctimas vulnerables.

Otro factor contributivo de la cibercriminalidad se relaciona con los efectos probatorios del anonimato cibernético. El anonimato en redes implica ocultar la identidad del cibercriminal y el lugar de conexión del mismo (Defensoría del Pueblo, 2023). Se trata, por tanto, de un factor que dificulta la acreditación y probanza del cibercrimen (Espinoza; 2022a).

Este carácter "anónimo" (Moron, 1999) provoca en la víctima la sensación, rayana con la certeza, de que la justicia penal no podrá dar con el responsable del ataque en su contra; la víctima siente que se enfrenta a un ser "invisible" frente a cuyos ataques sólo queda resignarse, por lo que pocas veces denuncian los hechos que se dan en su perjuicio.

Ahora, el reconocimiento de dificultades particulares en la persecución del cibercrimen no lleva necesariamente a desconocer que aquello sea posible en casos particulares (Reyna Alfaro, 2003) y en la medidas que las técnicas de investigación se apliquen adecuadamente. Sobre esto volveremos más adelante.

b) Asunción de riesgos vinculados a la mayor accesibilidad a las TIC's

La correlación entre el grado de accesibilidad a las TIC's, el crecimiento de la infraestructura digital y la exposición al cibercrimen se hace cada vez más notoria. El acceso de la población peruana al internet se duplico entre el 2010 al 2022, especialmente a partir del uso de los teléfonos digitales (Defensoría del Pueblo, 2023) y la irrupción del llamado *internet de las cosas,* lo que se ha visto reflejado en las estadísticas del cibercrimen.

Este nivel de exposición al riesgo de victimización se hace más crítico con relación a las víctimas particularmente vulnerables, especialmente menores de edad, que ven cómo es que los contactos interpersonales virtuales pueden ser aprovechados por el victimario

1 Sobre las tipologías propuestas en la doctrina penal, véase: Göppinger, H. (1975). *Criminología*. Reus, pp. 370 ss.; Kaiser, G. (1978). *Criminología*. Espasa Calpe, p. 94; De Rivacoba, M. (1982). *Elementos de criminología*. Universidad de Valparaíso, pp. 254-255; Neuman, E. (1984). *Victimología*. Editorial Universidad, pp. 56 ss.; Rodríguez Manzanera, L. (1995). *Criminología*. Porrúa, pp. 513 ss.; Solís Espinoza, A. (1988). *Criminología*, pp. 61 ss.; Aller, G. (2015). *El derecho penal y la víctima,* BdeF, pp. 29 ss.

para someter a la víctima. Se puede reconocer cómo es que el *child grooming* (especialmente el de tipo sexual) constituye el punto de partida para el desarrollo de conductas delictivas más gravosas, como el chantaje informático (Arocena, 2015).

c) Asunción de riesgos por contactos imprudentes o riesgosos. Vinculación del victimario con la víctima del cibercrimen (victim precipitation).

Los enfoques iniciales de la victimología —especialmente Mendelsohn y von Hentig— se centraron en examinar la vinculación entre víctima y victimario, esto es, la denominada *pareja penal* (Aller, 2015; Neuman, 1984). Esta vinculación se produce en el contexto particular del hecho criminal (Aller, 2015).

En efecto, aunque el espacio de cobertura de la victimología se haya extendido, no puede desconocerse que su objeto de estudio comprende necesariamente el análisis de las relaciones entre víctima y víctima (Kaiser, 1978). Este análisis comprende también —aunque no únicamente— la *victim precipitation* (Tamarit, 2006); es decir, la influencia de la víctima como causa generadora del hecho delictivo.

Ahora, los contactos imprudentes y riesgosos propiciados por la víctima pueden ser encontrados tanto en los ciberdelitos patrimoniales o económicos como en los ciberdelitos sociales, conforme a la clasificación acuñada por Miró Llinares (2013).

En ese contexto, dentro de los riesgos más comunes en el **cibercrimen patrimonial o económico** pueden mencionarse, entre otros, aquellos propios de las *compras on line* que pueden involucrar la entrega de datos bancarios que pueden ser objeto de utilización fraudulenta y la descarga de archivos informáticos peligrosos que propician actos de sustracción de información bancaria (Miró Llinares, 2013).

Por otro lado, respecto del **cibercrimen social** pueden mencionarse aquellos supuestos vinculados a la entrega o difusión de información personal que pueden dar lugar a un vasto espacio para la afectación de los intereses de la víctima del delito: *cyberstalking, child grooming, cyberbulling* (Miró Linares, 2013).

No es difícil reconocer que el desarrollo de conductas imprudentes o riesgosas por parte de la víctima podría derivar en la atribución del hecho a su propio costo. En estos casos, la *actuación a propio riesgo de la víctima* excluye la atribución del tipo penal objetivo del delito (Guarniz, 2023) y genera una brecha de impunidad que favorece al ofensor.

d) Riesgos derivados de la ausencia de percepción de la victimización.

En muchas ocasiones, el cibercrimen resulta imperceptible para su víctima (Arocena, 2015; Reyna Alfaro, 2002a), tanto por no identificar su victimización, por no reconocerse como tal o por no asignar al hecho un significado delictivo.

La invisibilidad del cibercrimen, como bien sostiene Herrera (2001), tendría su razón de ser en la "relatividad del espacio y tiempo informático", a través de la cual "en un juguetón parpadeo cibernético, el delincuente se inviste con los más absolutos atributos de intemporalidad y ubicuidad" (s/p).

7.2. La vulnerabilidad de la víctima en el cibercrimen

Este criterio constituye un aspecto fundamental para analizar la posición de la víctima del cibercrimen y determinar su nivel de exposición concreto a riesgo de victimización. Este riesgo de victimización, como indica García Pablos de Molina (2003), no debe ser genérico ni homogéneo, sino que debe ser *diferencial*, es decir, considerando las particulares de cada persona con relación a cada delito. En nuestra opinión, se trata del factor más significativo en el ámbito de la cibercriminalidad.

En este tópico procuraremos identificar aquellas circunstancias que inciden en el grado de vulnerabilidad de la persona y que le exponen al riesgo de cibercrimen.

a) Vulnerabilidad informática de la víctima del delito. Especial aplicación en la cibercriminalidad económica.

La no implementación de medidas de ciberseguridad genera riesgo de victimización al colocar a la persona (natural o jurídica) en situación de vulnerabilidad, al hacerla un *target* más atractivo para los cibercriminales que tendrán menos dificultades para ejecutar exitosamente sus manipulaciones informáticas. Esto es especialmente relevante respecto de las víctimas de los cibercriminales económicos.

Estas tipologías de ciberdelincuentes —como refiere Miró Llinares (2013)— se manifiestan a través de diversas formas de ataque que habilitan la obtención de información de la víctima que le permitan la obtención de ventaja económica: infección con virus, empleo de spyware y prácticas de *hacking*, por citar algunas de estas. La implementación de medidas de ciberseguridad podría contener (reducir) el riesgo de victimización.

En ese contexto, la verificación de ciertos elementos de la imputación objetiva (atribución del riesgo) del cibercrimen se encontrará vinculada a ciertos criterios de seguridad informática y de protección de datos personales (Guarniz, 2023).

Igualmente, Espinoza (2022b), precisa lo siguiente:

> En efecto, uno de los principios de la protección de datos personales es el principio de seguridad (artículo 9 de la Ley de Protección de Datos, Ley N.º 29733) en virtud del cual los entes públicos o privados que

> tienen acceso a datos personales deben implementar medidas de protección informática (p. 51).

Lo antes indicado, se reconoce con particular claridad en la configuración del delito de acceso ilícito (*hacking*) previsto en la Ley N.º 30096 (Ley de delitos informáticos) que incorpora —como condición para la verificación del tipo penal objetivo del delito— la exigencia de que el autor *vulnere las medidas de seguridad previstas por el titular del sistema informático afectado*. De este modo, si la víctima no implementó medidas de seguridad o contención informática, no será tutelada penalmente (Reyna Alfaro, 2002b; García, 2023; Rodríguez, 2023). La implementación de deberes de autoprotección en términos de seguridad informática es un tópico habitual en la doctrina penal sobre cibercrimen (Reyna Alfaro, 2022).

Los incidentes de cibercrimen suelen ser asociados con el nivel de seguridad informática que poseen las empresas o corporaciones atacadas, ello generará, como es evidente, desprestigio en la empresa atacada. Es por tal razón que un alto número de incidentes de seguridad informática son mantenidos en reserva por decisión de las propias víctimas (Herrera, 2001; Herrera, 2006; Morón, 1999; Reyna Alfaro, 2002a).

b) La vulnerabilidad general de la víctima del delito (vulnerabilidad victimal).

Los factores de vulnerabilidad general de la víctima del delito se reflejan también en el ámbito particular del cibercrimen. En ese sentido, los factores de vulnerabilidad victimal más habituales, como la edad y el género, serán replicables al plano de la cibervictimología.

No debe, sin embargo, ignorarse que existen sectores del cibercrimen que guardan poca relación con los factores de riesgo antes indicados. Me refiere particularmente a aquellos sectores del *computer crime* que se producen como formas de delincuencia ocupacional (De La Cuesta y Pérez, 2010; Magliona, 1999) al ser delitos cometidos generalmente por empleados de las mismas empresas afectadas. Sobre esta cuestión, las Naciones Unidas, en su Manual sobre prevención y fiscalización de los delitos relacionados con las computadoras (1997), llegó a la conclusión que el 90% de los delitos informáticos eran ejecutados por empleados de las empresas o instituciones afectadas (Reyna Alfaro, 2002a).

8. Dificultades de la victimología para el estudio de la víctima del cibercrimen

Ahora, sin perjuicio de haber reconocido y postulado algunas ideas iniciales que pueden ser de utilidad para el conocimiento de la victimología del cibercrimen, es oportuno hacer referencia a otros aspectos que dificultan el conocimiento acertado del cibercrimen y su víctima.

8.1. Cibercrimen y cifra oculta de la criminalidad

La "cifra oculta" que existiría en este sector de la criminal resulta un factor relevante para mantener el nivel de *desconocimiento* de las particularidades de la cibercriminalidad (Elías Puelles, 2022) a través de estadísticas reales que proporcionen información fidedigna particular sobre la víctima en estos delitos (Espinoza, 2022a)

Ya indicaba Middendorff que la cifra oculta de la criminalidad es "una nube gigantesca e impenetrable" (1961, p. 51). Las dificultades del sistema de administración de justicia para trasladarse desde lo desconocido hacia lo conocido en el plano de la criminalidad han llevado a autores como Exner a denominar a la cifra oculta como *la cruz de la estadística criminal* (citado por Middendorff, 1961; también, Kaiser, 1978).

La "cifra oculta" de la criminalidad constituye, así, evidencia de la "eficacia" del ofensor (Solís, 1988) y, evidentemente, también de la ineficacia e incapacidad del sistema de administración de justicia penal para proporcionar información idónea para procurar una reacción penal estatal idónea para enfrentar la criminalidad.

La "cifra oculta" en el terreno de la criminalidad informática, pese a carecer de mayores estudios criminológicos o de estadísticas sobre victimización que permitan fijar su proporción, el nivel de sus daños (similares, Meneses Gonzáles y Meneses Ochoa, 2024) así como estudiar el movimiento de la criminalidad (Marcó del Pont: 2006), es considerada unánimemente por la doctrina de gran entidad (González, 2000; Morón, 1999). Ahora, es también verdad que esta premisa (dañosidad significativa del cibercrimen) es aún insuficiente para proporcionar bases certeras y absolutamente fiables para el estudio de este fenómeno delictivo.

Este aspecto (el conocimiento de los índices de criminalidad) —como ha resaltado Serrano Maíllo (2009)— se relaciona con una de las funciones básicas de la Criminología: la medición del delito, de allí su particular importancia en esta parcela de la criminalidad.

Ahora, el estudio de la denominada "cifra oculta" de la criminalidad es una cuestión que se encuentra cercanamente relacionada al estudio de las víctimas y obliga, entre otros aspectos, a examinar los motivos que le impulsaron a no hacer de conocimiento los hechos cometidos en su perjuicio (Göppinger, 1975; Neumann, 1984).

8.2. Dificultades probatorias, ineficacia de la persecución penal y victimización secundaria

Una de las razones que contribuyen a mantener ocultos los supuestos de cibercrimen es la especial dificultad que reviste su acreditación dentro del proceso

penal. El riesgo de impunidad es claramente reconocible y genera un riesgo colateral de victimización secundaria atribuible al sistema de administración de justicia penal.

En efecto, una de las principales características del cibercrimen es su elevado nivel de tecnicidad, que dificultan su identificación, persecución y acreditación (Barrio, 2017; Mata y Martín, 2003). Estas dificultades probatorias, como advierte Espinoza (2022b) guardan también relación con el grado de vulnerabilidad de las redes sociales y con los riesgos de adulteración de la evidencia en esos espacios de la vida moderna.

Estas circunstancias provocan un riesgo severo de impunidad del cibercrimen (Reyna Alfaro, 2002a) y ello puede generar —como ya hemos adelantado— un riesgo de victimización secundaria que se transforma en un desincentivo para comunicar la victimización sufrida a las autoridades competentes. Si la víctima del cibercrimen recurre al sistema de administración de justicia penal y no obtiene tutela procesal por no emitirse declaración judicial de certeza de la victimización en su perjuicio, no solo verá defraudada sus expectativas, sino que probablemente sufra efectos reputacionales y legales derivados de la exposición del incidente cibernético al escrutinio público, además del incremento de la pérdida patrimonial asociada a los costos económicos propios de la activación del sistema de administración de justicia.

En cuanto a los efectos reputacionales, podemos indicar que las víctimas del cibercrimen, especialmente las personas jurídicas, cuando exponen los hechos que le han afectado, sufrirán una auténtica publicidad o exposición negativa (Adamski, 1999; De La Cuesta y Pérez, 2010; Reyna Alfaro, 2002a; Meneses Gonzáles y Meneses Ochoa, 2024), pues la victimización sufrida podría guardar relación con la fortaleza y capacidad de sus medidas de ciberseguridad.

Pero no es solo que la victimización secundaria se expresa en términos de efectos reputacionales negativos, sino que podrían generar impactos legales derivados de la verificación de la no implementación de obligaciones de ciberseguridad en el caso de personas jurídicas y ello podría generarles responsabilidad frente a terceros (especialmente sus clientes). En ese contexto, conviene recordar que el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad aplicables a las entidades del sistema financiero y administradoras privadas de fondos de pensiones (Resolución SBS N.º 504-2021) describe una serie de medidas mínimas de ciberseguridad que, aunque no son mandatorias, fijan un marco de diligencia debida que podría considerarse un estándar aplicable al sector financiero (Espinoza, 2023).

Ahora, a modo de *disclaimer* debemos incorporar una precisión relevante: poner énfasis en las dificultades probatorias propias del cibercrimen no supone que se atribuya a los órganos a cargo de su persecución y sanción algún tipo de responsabilidad por ineficacia. En efecto, aunque en el pasado (2002) resaltábamos los riesgos de ineficacia del sistema de administración de justicia penal derivados de la ausencia de criterios de especialización en la persecución del delito, desde entonces esa circunstancia ha ido variando progresivamente. Desde el 2005 se cuenta con una División Policial de Delitos de Altas Tecnologías y desde el 2020 se cuenta con una unidad de acompañamiento técnico al trabajo fiscal de persecución del cibercrimen y con fiscalías especializadas en cibercrimen (Defensoría del Pueblo, 2023; Vílchez Limay, 2025). En todo ello ha tenido especial impacto la adopción del Convención de Budapest sobre Ciberdelincuencia (2001) que establece pautas asociadas a la investigación del cibercrimen (Petrone, 2014) y que viene propiciando la propalación de diligencias de investigación penal tecnológicas (Bustamante, 2023) en nuestros ordenamientos procesales.

9. Conclusión y epílogo

En las líneas precedentes hemos revisado parte de los problemas que afectan a la victimología y los hemos abordado desde el prisma particular que proporciona el cibercrimen. En este propósito, hemos ido advirtiendo una serie de falencias estructurales que inciden directamente en la política criminal orientada a la prevención de esta expresión de la criminalidad.

En muchos de mis trabajos he tratado de insistir en la necesidad de enfrentar la tradición anti-empírica que predomina aún en el estudio de la criminalidad (Reyna Alfaro, 2022a), lo que provoca que las decisiones de política jurídica resulten respuestas intuitivas, especulativas y, por ello, poco acertadas. Insistimos en la necesidad de priorizar el estudio criminológico y victimológico fundado en clave empírica.

Y aunque las soluciones a los problemas parecieran no estar aún a la vista, no puede renunciarse a la pretensión científica de generar *masa crítica* que pueda servir para generar consensos que permitan la construcción de una auténtica *victimología del cibercrimen*.

Lista de referencias

Adamski, A. (1999). Crimes related to the computer network. Threats and opportunities: A criminological perspective. En *Five issues in European Criminal Justice: Corruption, Women in the Criminal Justice System, Criminal Policy Indicators, Community Crime Preventor and Computer Crime*. European Institute for Crime Prevention and Control, HEUNI.

Alarcón Arias, P. (2019). Compliance y ciberseguridad. En Forero, J.; Escobar, S.; Ibáñez, J.; Silva, M.; Alarcón, P. (coords.), *Ciberespacio, ciberseguridad y ciberjusticia en la era digital*. Universidad del Rosario.

Aller, G. (2015). *El derecho penal y la víctima*. BdeF.

Arocena, G. (2015) *Ataques a la integridad sexual*. Astrea.

Barrio Andrés, Moisés (2017). *Ciberdelitos: Amenazas criminales en el ciberespacio* (Madrid) Editorial Reus.

Beck, Ulrich (2006). *La sociedad del riesgo*. Paidós.

Bramont Arias Torres, L. A. (1987). *El delito informático en el Código Penal peruano*. Fondo Editorial de la Pontificia Universidad Católica del Perú.

Bustamante Rúa, M. (2023). *Cibercriminalidad e investigación penal tecnológica*. Palestra.

Defensoría del Pueblo (2017). *La ciberdelincuencia en el Perú: Estrategias y retos del Estado, informe defensorial N.º 001-2023-DP/ ADHPD*.

De La Cuesta Arzamendi, J. L. & Pérez Machío, A. I. (2010). Ciberdelincuentes y cibervíctimas. En De la Cuesta, J. L, (dir.), *Derecho Penal informático*. Civitas.

De Rivacoba, M. (1982). *Elementos de criminología*. Universidad de Valparaíso.

Durán Valladares, R. (2002). *Cyber-delito o delito de ordenadores*.

Elbert, C. (2007). *Inseguridad, víctimas y victimarios*. BdeF.

Elías Puelles, R. (2022). Suplantación de identidad en el Perú. En Caro Coria, D. & Reyna Alfaro, L. M. (dirs.). *Ciberseguridad, cibercrimen y nuevas tecnologías*. Derecho Global.

Escobar Beltrán, S.; García Carreño, A. & Jiménez Guacaneme, F. (2019). Internet y juicios paralelos. En Forero, J.; Escobar, S.; Ibáñez, J.; Silva, M.; Alarcón, P. (coords.), *Ciberespacio, ciberseguridad y ciberjusticia en la era digital.* Universidad del Rosario.

Eser, A. (1998). Sobre la exaltación del bien jurídico a costa de la víctima. En Eser, A., *Temas de Derecho Penal y Procesal Penal*. Idemsa.

Espinoza Calderón, V. (2022a). *Delitos informáticos y nuevas modalidades delictivas.* Instituto Pacífico.

Espinoza Calderón, V. (2022b). *Valoración probatoria de los contenidos de redes sociales.* AC Ediciones.

Espinoza Calderón, V. (2023). El delito de fraude informático. En Espinoza, V. (coord.), *Cibercriminalidad y delitos informáticos*. Instituto Pacífico.

Faraldo Cabana, P. (2009). *Las nuevas tecnologías en los delitos contra el patrimonio y el orden económico*. Tirant lo Blanch.

García León, A. (2023). Análisis del tipo de acceso ilícito. En Espinoza, V. (coord.), *cibercriminalidad y delitos informáticos.* Instituto Pacífico.

García Pablos de Molina, A. (2003). *Tratado de Criminología*. Tirant lo Blanch.

Göppinger, H. (1975). *Criminología*. Reus.

Grabosky, P. (2015). *Cybercrimen*. Oxford University Press.

Guarniz Rodríguez, M. (2013). Sobre la posibilidad de imputacion del hecho a la víctima del phishing. En Espinoza, V. (coord.), *Cibercriminalidad y delitos informáticos.* Instituto Pacífico.

Gutiérrez Francés, M. (1991). *Fraude informático y Estafa*. Ministerio de Justicia.

Herrera Moreno, M. (2001). El fraude informático en el derecho penal español. *Actualidad Penal*, (39), 925-964.

Herrera Moreno, M. (2006). Tema 3: victimación. Aspectos generales. En Baca, E; Echeburúa, E.; Tamarit, J. (coords.). *Manual de victimología.* Tirant lo Blanch.

Holt, T.; Smirnova, O.; Chua, Y. T. (2016). *Data thieves in action. Examining the international market for stolen personal information*. Palgrave Mcmillan.

Jiménez Herrera, J. C. (2017). *Manual de Derecho Penal Informático*. Jurista Editores.

Kaiser, G. (1978). *Criminología.* Espasa Calpe.

Magliona Markovicth, C.; López Medel, M. (1999). *Delincuencia y fraude informático*. Editorial Jurídica de Chile.

Marcó del Pont, L. (2006). *Manual de Criminología.* Ediciones Jurídicas.

Mata y Martín, R. (2003). *Delincuencia informática y derecho penal*. Hispamer.

Meneses Gonzáles, B. & Meneses Ochoa, J. (2024). *La cibercriminalidad*. UPSA Ediciones.

Middendorff, W. (1961). *Sociología del delito*. Revista de Occidente, 46-47.

Miró Llinares, F. (2013). *Cibercrimen, cibercriminales y cibervíctimas*. Universitat Oberta de Catalunya. https://openaccess.uoc.edu/bitstream/10609/70006/4/Delincuencia%20y%20TICs_M%C3%B3dulo%202_Cibercrimen%2C%20cibercriminales%20y%20ciberv%C3%ADctimas.pdf).

Miró Llinares, F. (2015). That cyber routine, that cyber victimization: profiling victims of cybercrime. En Smith, R.; Chak Chung, R. & Yiu Chung, L. (eds.), *Cybercrime risks and responses. Eastern and Western Perspectives*. Palgrave Mcmillan.

Morón Lerma, E. (1999). *Internet y Derecho penal: hacking y otras conductas ilícitas en la red*. Aranzadi.

Neuman, E. (1984). *Victimología*. Editorial Universidad.

Petrone, D. (2014). *Prueba informática*. Ediciones Didot.

Reyna Alfaro, L. M. (2002a). *El delito informático. Aspectos criminológicos, dogmáticos y de política criminal*. Jurista Editores.

Reyna Alfaro, L. M. (2002b). Los delitos informáticos en el Código Penal peruano. En Chiara, E. (comp.), *Derecho informático y comercio electrónico*. Facultad de Derecho y Ciencias Politicas de la UIGV.

Reyna Alfaro, Luis Miguel (2003). El intrusismo informático ¿legalidad penal o impunidad?: Reflexiones a partir del caso argentino del "X—Team". En *El Derecho Penal*. Universidad Católica Argentina.

Reyna Alfaro, L. M. (2006). La víctima en el sistema penal. En AA.VV, *La víctima en el sistema penal*. Grijley.

Reyna Alfaro, L. M. (2016). Criminalidad informática, crimen organizado e internacionalización del delito. En Zuñiga, L. (dir.). *Ley contra el crimen organizado (Ley N.º 30077)*. Instituto Pacífico.

Reyna Alfaro, L. M. (2022). Prevención del cibercrimen, ciberseguridad y *compliance* digital. En Caro Coria, D. & Reyna Alfaro, L. M. (dirs.), *Ciberseguridad, cibercrimen y nuevas tecnologías*. Derecho Global.

Reyna Alfaro, L. M. (2022a). Sin criminología no hay paraíso: seis reflexiones sobre las razones por las que debes estudiar criminología. En Vidaurri, M. & Esquivel, A. (coords.), *Cartas a jóvenes estudiantes de criminología*. Tirant lo Blanch.

Rodríguez Rocha, L. (2023). El delito de acceso ilícito a los sistemas informáticos. En Espinoza, V. (coord.), *Cibercriminalidad y delitos informáticos*. Instituto Pacífico.

Rodríguez Manzanera, L. (1995). *Criminología*. Porrúa.

Serrano Maíllo, A. (2009). *Introducción a la criminología*. Dykinson.

Silva Sánchez, J. M. (1993). La consideración del comportamiento de la víctima en la teoría jurídica del delito. En AA.VV, *La victimología*. Consejo General del Poder Judicial.

Silva Sánchez, J. M. (2001). *La Expansión del Derecho penal. Aspectos de la política criminal en las sociedades postindustriales* (2.ª ed.). Civitas.

Solís Espinoza, A. (1988). *Criminología*. DESA.

Tamarit Sumalla, J. (2006). Tema 1: la victimología. Cuestiones conceptuales o metodológicas. En Baca, E.; Echeburúa, E. & Tamarit, J. (coords.), *Manual de victimología*. Tirant lo Blanch.

Valls Prieto, J. (2017). *Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial*. Dykinson.

Vidaurri Aréchiga, Manuel (2016). *Bases generales de criminología y política criminal*. Oxford University Press México.

Vílchez Limay, R. (2025). El registro remoto sobre equipos informáticos. En Caro Coria, D.; Reyna Alfaro, L. & Elías Puelles, R. (dirs.), *Ciberseguridad, cibercrimen y AI Legal Tech*. Derecho Global.

Villavicencio Terreros, F. (2000). *Introducción a la criminología*. Grijley.

Von Hentig, H. (1962). *Estudios de psicología criminal II*. Espasa Calpe.

Von Hentig, H. (1972). *El delito II*. Espasa Calpe.