Revista Española
de Investigación Criminológica

2024, vol22(2) e969
https://doi.org/10.46381/reic.v22i2.969

Editorial Número Especial
TIC y Criminalidad

Steven Kemp[1*] y Abel González[2]

1. Departamento de Derecho Público, Universitat de Girona
2. Departamento de Criminología, Universidad a Distancia de Madrid
* Correspondencia a steven.kemp@udg.edu

La relación entre las TIC y la Criminalidad

Cuando Ray Tomlinson envió el primer correo electrónico en 1971, no podía imaginar la magnitud de los cambios tecnológicos y sociales que iban a tener lugar en las cinco décadas siguientes. No es exagerado afirmar que, en estos más de 50 años, las Tecnologías de la Información y la Comunicación (TIC) han tenido un impacto en las interacciones humanas que se dan en todas las esferas de la vida. Por ejemplo, nosotros estamos escribiendo este editorial desde diferentes lugares de España en un documento compartido mediante computación en la nube con revisión de ortografía automatizada e instantánea. Cuando terminemos, el texto formará parte de una revista electrónica alojada en un servidor alquilado que vosotros podéis leer gratis en vuestros dispositivos hechos con microchips asiáticos y software americano. Un día normal en el mundo digital global.

En este contexto de rápida transformación tecnológica y social, la criminalidad y todas las organizaciones e instituciones relacionadas con la prevención de este fenómeno social también han cambiado. En este sentido, las innovaciones criminológicas y su impacto en la delincuencia pueden clasificarse *grosso modo* en tres categorías: nuevas formas de delincuencia, el uso de las TIC en elementos esenciales de la delincuencia tradicional o en la transversalidad de las TIC en diversos elementos no esenciales de la delincuencia tradicional.

En primer lugar, han aparecido nuevos tipos delictivos que no pueden existir sin las TIC dado que su objetivo es impedir el correcto funcionamiento de los propios sistemas informáticos. Los ejemplos más conocidos serían la difusión del malware tipo *ransomware* o los ataques *DDoS*, que han dado lugar a diversos casos mediáticos como el intento de extorsión al Hospital Clínic de Barcelona[1] o el bloqueo de las páginas web de instituciones españolas[2]. En segundo lugar, otros tipos delictivos se han adaptado o potenciado con el uso de nuevas tecnologías, siendo las estafas el ejemplo más claro debido a que se han convertido en una amenaza global

[1] Para más información sobre el caso, véase: https://www.clinicbarcelona.org/prensa/ultima-hora/ciberataque-al-hospital-clinic-de-barcelona

[2] Véase, por ejemplo: https://www.dsn.gob.es/ca/actualidad/seguridad-nacional-ultima-hora/nacional-ciberseguridad-5

que genera pérdidas de miles de millones alrededor del mundo; o el acoso, que ya no respeta barreras físicas o temporales; e incluso, el espionaje, en el que hoy en día no hace falta que un agente de inteligencia se infiltre físicamente en organizaciones hostiles. Y, en tercer lugar, desde una perspectiva más amplia, podemos observar cómo las TIC forman parte de la mayoría de las actividades delictivas sin ser centrales en la vertiente comisiva, como por ejemplo, la utilización de la tecnología para facilitar la comunicación, la organización o los flujos financieros entre delincuentes.

Como consecuencia de esta tecnificación del crimen, las organizaciones e instituciones implicadas en la prevención y respuesta al delito han tenido que adaptarse de diversas maneras. Por un lado y en términos jurídicos, los legisladores han tipificado nuevas conductas, muchas veces debido a iniciativas legislativas supranacionales como el Convenio sobre Cibercriminalidad del Consejo de Europa (2001). Por otro lado, dado que las TIC permiten mayor transnacionalidad en la delincuencia, las instituciones encargadas de la investigación del crimen han tenido que promover mecanismos que faciliten la cooperación transfronteriza. Un elemento central a esta cooperación son las evidencias digitales, que tienen un peso cada vez mayor en las investigaciones y cuya recopilación y análisis requiere capacidades y herramientas específicas. No obstante, las evidencias digitales muchas veces están en manos de empresas privadas, por lo que también se han tenido que fomentar mecanismos de colaboración con organizaciones empresariales, que, en algunos casos, pueden no apreciar los incentivos económicos para colaborar en la persecución de la delincuencia.

Un aspecto importante en el análisis de esta fenomenología criminológica es que las organizaciones privadas también tienen un creciente rol en la prevención del delito en la era digital, porque parte de la responsabilidad para prevenir la criminalidad cometida mediante las TIC corresponde a las empresas tecnológicas que gestionan los espacios virtuales y los flujos de datos que ocurren en ellos. La Unión Europea reconoce esta responsabilidad y estipula ciertas obligaciones en la tercera versión de la Directiva de Servicios de Pagos UE (2023) y la Ley de Servicios Digitales UE (2022).

Como se puede apreciar mediante los ejemplos de esta breve introducción, la relación simbiótica entre las TIC y la criminalidad es profunda y, por consiguiente, la comunidad criminológica internacional no tardó en comenzar a analizar la relación entre sus objetos de estudio y los diversos cambios tecnológicos y sociales de la era digital.

El creciente corpus de investigación criminológica sobre TIC y Criminalidad

Al principio, una gran parte del debate criminológico se centraba en las definiciones de las nuevas formas de criminalidad, así como las similitudes y diferencias entre esta y la criminalidad tradicional. Sobre todo, definir el muy conocido término "*cybercrime*" ha ocupado múltiples autores. Dos definiciones parecidas y frecuentemente citadas de principios del presente siglo delimitaron una categoría muy amplia: Loader y Thomas (2000, p. 3) lo consideraban "actividades mediadas por computadoras que son ilegales o consideradas ilícitas por ciertas partes y que pueden llevarse a cabo a través de redes electrónicas globales", mientras que David Wall (2001, p. 2) decía que se refiere simplemente a "un comportamiento dañino que está relacionado de alguna manera con una

computadora". Respecto a la diferencia entre la criminalidad mediada por las herramientas digitales y la criminalidad tradicional, una analogía basada en el vino se ha empleado para ilustrar diferentes perspectivas. En este sentido, Peter Grabosky (2001) conceptualizaba al cibercrimen como vino viejo en botellas nuevas para destacar las similitudes con la criminalidad ya conocida. En cambio, Wall (1999) preguntaba si era vino nuevo sin botella, así destacando las nuevas formas de criminalidad creadas con las TIC y el carácter transnacional del ciberespacio.

La criminología del mundo hispanohablante tardó un poco más en entrar en este debate. Probablemente no fue hasta la publicación del libro seminal del Profesor Fernando Miró Llinares (2012) que se podría hablar de un interés científico criminológico en la relación entre las TIC y criminalidad. En esta obra, el autor matizó las definiciones mencionadas arriba. Por un lado, Miró definió el cibercrimen "como cualquier delito en el que las TIC juegan un papel determinante en su concreta comisión" (pág 44), es decir, que no es suficiente que las TIC hayan sido simplemente un elemento secundario, sino que tienen que condicionar la actividad en alguna medida. Esta posición ha sido respaldada más recientemente por criminólogos internacionales (Lusthaus, 2024). Por otro lado, el Profesor Miró Llinares precisó que el cibercrimen "es vino, pero se bebe de otra forma" (pág 144), ya que el crimen, como todo hecho social, es distinto en internet.

Una cuestión central al desarrollo de estos debates en la actualidad es la impregnación de las TIC en todo momento de la vida cotidiana, cosa que dificulta distinguir entre las actividades mediadas por las TIC y las actividades analógicas. Por ejemplo, si hoy en día tenemos un dispositivo conectado a Internet al alcance de la mano en cada momento, ¿existe *bullying* o suplantación de identidad sin un elemento "ciber"? Esta discusión definicional debe continuar para sentar las bases para el análisis empírico de la relación entre las TIC y la criminalidad.

En todo caso, desde cualquiera de las perspectivas anteriormente mencionadas, está claro que los términos cibercrimen o cibercriminalidad engloban una gran cantidad de conductas de índole muy diversa y, por tanto, es necesario algún tipo de categorización para guiar las líneas de investigación. En la literatura, se pueden identificar tres principales formas de categorizar la cibercriminalidad. Primero, Wall delimitó cuatro agrupaciones legales denominadas "ciberintrusiones, ciberengaños y robos, ciberpornografía, y ciberviolencia" (2001, pp. 3-7). En segundo lugar, se puede identificar una serie de categorizaciones que tienen relación con el rol del sistema informático o los datos. Por ejemplo, McGuire y Dowling, La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), y Miró Llinares diferenciaron entre delitos en los que los sistemas o los datos digitales son esenciales para su comisión y aquellos en los que las TIC facilitan la ejecución de ilícitos ya existentes en su versión analógica (McGuire & Dowling, 2013; Miró Llinares, 2012; United Nations Office on Drugs and Crime, 2013). Tercero, Miró Llinares también analizaba los cibercrímenes en función de si el móvil u objetivo del infractor era económico, social (daños no económicos contra individuos), o político (motivos ideológicos).

Uno de los objetivos principales de reflexionar sobre la naturaleza de la criminalidad que tiene lugar mediante las TIC y las similitudes y diferencias entre esta y la criminalidad tradicional es estudiar la aplicabilidad de las teorías criminológicas existentes. A día de hoy, se puede encontrar una diversidad de estudios que han analizado la cibercriminalidad desde los fundamentos de la escuela clásica, la teoría de la elección racional, la perspectiva de las actividades cotidianas, la teoría del aprendizaje social, las teorías de la frustración, la teoría del autocontrol, las técnicas de neutralización, o la criminología feminista, entre otras (Yar & Steinmetz, 2023). En general, los principios

básicos de estas perspectivas teóricas tradicionales proporcionan un marco explicativo que ayuda a comprender el papel de las TIC en el comportamiento desviado. A modo de ejemplo, se ha analizado la manera en que los espacios virtuales pueden proporcionar un lugar para desahogar tensiones en detrimento de terceros, o cómo estos espacios sirven para eliminar las barreras de aprendizaje para emprender una carrera de ciberestafador, o el modo en que facilitan el encuentro entre el agresor y la víctima.

A su vez, entender mejor la criminalidad en la que las TIC juegan un papel determinante y los factores asociados con la victimización y su impacto puede ayudar en el diseño de estrategias de prevención. Con base en un marco de las teorías de la tensión, las actividades cotidianas y la criminología feminista se podría abordar las siguientes preguntas con implicaciones para la prevención: ¿por qué los hombres tienen mayor propensión a compartir imágenes digitales íntimas de sus exparejas como forma de venganza? ¿Qué impacto tiene sobre las víctimas la difusión global de estas imágenes? ¿Cómo se puede limitar la difusión? O, desde el prisma de la escuela clásica, la criminología ya ha señalado que, en términos instrumentales, los efectos disuasorios de las penas y las sanciones dependen de la probabilidad de ser identificado y efectuarse el castigo, más que en la dureza de este. Por consiguiente, las instituciones de política criminal deben tener un interés en conocer las tasas de esclarecimiento de la cibercriminalidad y los factores que impiden una mayor capacidad de actuación. En síntesis, el comportamiento desviado en línea y las respuestas al mismo tienen particularidades respecto a sus homólogos de antes de la expansión de las tecnologías digitales, pero muchas de las explicaciones tradicionales tienen cierta aplicabilidad que puede guiar la investigación empírica sobre las TIC y la criminalidad en la actualidad.

Para acabar este breve resumen de la investigación internacional sobre TIC y criminalidad, queremos mencionar que, además de estas líneas de investigación sobre la cibercriminalidad en los sentidos más estrictos, existe un gran corpus de estudios que analizan la relación entre las TIC y los objetos de estudio criminológico desde una perspectiva más amplia. Por ejemplo, enlazando con el caso comentado en el párrafo anterior, se han producido diversos cambios organizativos y tecnológicos en las instituciones policiales o carcelarias en la época digital y los estudios empíricos han analizado las implicaciones de ellos. Del mismo modo, hay una larga tradición criminológica de estudiar la opinión pública acerca de la política criminal y es indudable que las redes sociales y la mensajería instantánea han tenido algún tipo de impacto en la configuración de las opiniones de la ciudadanía, tal y como nos indica la literatura incipiente.

En el contexto hispanohablante, las investigaciones empíricas criminológicas sobre las diferentes vertientes de la relación entre las TIC y la criminalidad han avanzado a un ritmo menor. En la Revista Española de Investigación Criminológica, salvo error por nuestra parte, antes de este número especial, tan solo siete artículos han tratado alguno de los temas mencionados en los párrafos anteriores. Algo sorprendente teniendo en cuenta el impacto de las TIC en la criminalidad y las organizaciones implicadas en el control de la misma. Aun así, en este pequeño grupo podemos apreciar un interés sobre todo en la cibercriminalidad social, que fue el objeto principal de los estudios de González García y Campoy Torrente (2018), de Miró Llinares (2013), de Pascual y compañeros (2017), y de Villacampa y Pujols (2017), y fue una cuestión entre otras en el estudio de Grijalva Eternod (2023). Asimismo, Rodríguez Ferrández y compañeros analizaron la eficacia de una intervención preventiva con adolescentes respecto a esta categoría de cibercriminalidad (Rodríguez Ferrández

et al., 2017). Por su parte, y sin centrarse específicamente en la cibercriminalidad, Moreno-Ruiz y compañeros examinaron el posible papel de las redes sociales en la violencia física en la escuela (Moreno-Ruiz et al., 2024).

Más allá de la REIC, se puede apreciar un interés creciente en los estudios empíricos sobre víctimas en el contexto español (para diversos ejemplos, véase Agustina et al., 2020 o Kemp, 2024), pero destaca el vacío empírico en cuanto a los infractores, la prevención, o el uso de las tecnologías de la comunicación en las instituciones de política criminal. Por experiencia propia, podemos afirmar que algunos de los principales factores que explican la falta de avances en estas líneas en España son las debilidades de los datos públicos, la poca disposición de las instituciones del sistema penal a trabajar en estudios académicos, y las escasas fuentes de financiación para producir datos primarios. En este entorno poco favorable nace este número especial, lo que resalta aún más el mérito de los estudios que lo componen al avanzar el conocimiento criminológico sobre un tema que indudablemente aumentará en trascendencia en los próximos años.

Los estudios incluidos en este número especial

El primer artículo de este número especial utiliza una base de datos de 133.777 personas para examinar los cambios sociales relacionados con las tecnologías digitales y la criminalidad en el sur global. En este sentido, Figueiredo Alves Silva y Miro-Llinares (2024) han analizado datos de Brasil que actualmente sería impensable conseguir de las instituciones públicas en España, tal y como se ha expuesto en la sección anterior. El análisis indica que la digitalización de la sociedad del sur de Brasil no solo está asociada a un aumento de la cibercriminalidad, sino también tiene relación con una bajada en los delitos de daños a la propiedad en el espacio físico. Para explicar estos resultados, los autores resaltan la importancia de las nuevas formas de socialización entre adolescentes para aumentar la exposición a riesgos de victimización mediante las tecnologías digitales y, a la vez, para configurar nuevos hábitos sociales que reducen la probabilidad de participar en la delincuencia callejera. Según destacan, la digitalización de las interacciones sociales entre los jóvenes impacta las oportunidades delictivas tanto en el espacio físico como en el espacio virtual, cosa que se ve reflejada en las tendencias en las estadísticas policiales. Asimismo, este cambio en las tendencias delictivas fue agudizado gracias a la aceleración de ciertas tendencias digitales relacionadas con la pandemia del Covid-19, tal y como encuentran los autores.

Las implicaciones de estos hallazgos son múltiples y variadas. Entre ellas, los autores destacan las mayores dificultades que supone la medición de la cibercriminalidad en comparación con algunos otros tipos delictivos. Cuando un fenómeno criminal presenta una alta cifra negra o dificultades para su medición, resulta más difícil asignar recursos para combatirlo. En este sentido, se resalta la necesidad de tener unidades policiales con conocimientos profundos de las nuevas formas de criminalidad. Por otro lado, Figueiredo Alves Silva y Miro-Llinares reflexionan sobre cómo la digitalización de las interacciones está cambiando los hábitos sociales, sobre todo respecto a los jóvenes. No obstante, los nuevos hábitos no se distribuyen de forma homogénea entre este grupo demográfico, por tanto, para entender mejor la victimización en el ciberespacio, deberíamos conocer la relación entre el uso de tecnologías de internet y victimización.

En el segundo artículo de este número, Jordá y compañeras (2024) analizan unos lugares virtuales que han fomentado un gran desplazamiento delictivo: Los criptomercados ilícitos de tráfico de drogas en la DarkWeb. El aumento de los criptomercados se explica por los diversos beneficios que ofrecen para los vendedores tanto como los compradores, por ejemplo, relacionado con el anonimato, la calidad del producto, o la ausencia de violencia. Para obtener una comprensión integral de estos lugares digitales, los autores realizan un estudio exploratorio sobre las características de una muestra de 18 criptomercados. En primer lugar, se analizan las características de los criptomercados en términos de, por ejemplo, la cantidad de oferta, el número de interacciones de los usuarios o el método de acceso. En segundo lugar, describen las características de las ventas, incluyendo la fianza del vendedor y el tipo de pago. En tercer lugar, examinan las diversas formas de entrega empleadas.

La exploración de todas estas características permite a los autores extraer múltiples conclusiones sobre los criptomercados, que concuerdan con la literatura internacional. Una de ellas es la importancia que tiene la confianza para configurar todos los elementos de estos mercados. Otra conclusión destacable tiene que ver con la fase de entrega como momento de mayor inseguridad para el anonimato de los compradores. En este sentido, las conclusiones tienen implicaciones prácticas claras para las intervenciones de las organizaciones que luchan contra el tráfico de drogas en línea. Por un lado, reducir la confianza percibida en estos ciberlugares los hace menos atractivos para los usuarios y así se puede reducir los beneficios para los administradores y los vendedores. Por otro lado, la detección de las entregas puede dar inicio a investigaciones sobre los usuarios.

Cerezo Domínguez y García Cornejo (2025) exploran el fenómeno de *cyberstalking* en parejas juveniles a partir de los datos recogidos en el sistema VioGén de la Secretaría de Estado de Seguridad (denuncias recogidas en las que las víctimas son menores de 25 años). Este estudio se centra, en concreto, en el abuso en el noviazgo en parejas jóvenes. El objetivo principal es identificar características nuevas y/o llamativas del *cyberstalking*, más allá del análisis de la prevalencia de este fenómeno. En la mayoría de los casos analizados ocurren conductas tanto online como offline, y el *cyber dating abuse* se encontró exclusivamente en solo el 5,2% de los casos. Los resultados muestran que la aparición o el aumento de las conductas abusivas ocurrió después de la ruptura de la relación en casi un tercio de los casos estudiados. Asimismo, se encontraron una diversidad de conductas online como amenazas, acoso, insultos y control. Otra parte del análisis se centró en los medios más comunes para estas conductas, siendo los mensajes (41,5%), las llamadas telefónicas (25,5%) y las redes sociales (17,1%) los medios utilizados. En otro orden de cosas, se concluye que el sistema jurídico-penal responde principalmente con medidas como la prohibición de acercamiento y comunicación con la víctima (85% de los casos analizados). Y lo más interesante es que se identificaron variables presentes no habituales en las relaciones de pareja juveniles, como la convivencia y los hijos en común. El estudio tiene limitaciones debido a que solo se obtuvo información de mujeres jóvenes que denunciaron, y la información en el sistema VioGén a veces es incompleta, pero esta investigación sienta las bases para que futuros estudios puedan profundizar en el análisis de las respuestas del sistema jurídico-penal ante las conductas desviadas en línea.

El estudio de Erades-Pérez y Sitges Macià (2025) también aborda el tema de la cibervictimización, pero centrándose sobre todo en las reacciones de las víctimas. Mediante el análisis de respuestas de los 1.005 participantes de España en la encuesta Eurobarómetro 92.2, las autoras pretenden responder a tres preguntas de investigación relacionadas con las preocupaciones que

genera la cibervictimización y la denuncia de experiencias de victimización. Respecto a las denuncias, se identifica una alta cifra negra que tiene relación con el bajo conocimiento del proceso de denunciar. Tal y como subrayan las autoras, estos resultados indican que es necesario agilizar el proceso de denuncia en España, permitiendo, por ejemplo, denuncias por internet.

Con relación a la preocupación, por un lado, se encuentra una correlación positiva con la preocupación y el conocimiento sobre ciberdelitos y la victimización previa. No obstante, dado la naturaleza transversal de la encuesta, las estimaciones no permiten conocer el orden de las variables, es decir, si la mayor preocupación se debe al mayor conocimiento de la cibercriminalidad o viceversa. Por el otro lado, la encuesta preguntaba explícitamente sobre algunos comportamientos como respuesta a preocupaciones por la seguridad en línea. Los resultados del estudio indican que la mayoría de los respondientes manifestaron adoptar respuestas pasivas-evitativas, es decir, limitaban el uso de herramientas digitales ante preocupaciones. Las autoras subrayan que la falta de conocimientos sobre ciberdelitos y cómo prevenirlos puede hacer que las personas eviten actividades en lugar de implementar medidas de prevención de forma activa.

Por su parte, Díaz Ortega y compañeros (2025) analizan cómo las redes sociales se han convertido en un espacio para la reacción social frente al delito y han modificado las formas en las que la opinión pública se informa y expresa. A través de una revisión sistemática, los autores identifican tres aspectos clave: 1. La transformación de la opinión pública, en la que las redes sociales permiten una rápida difusión de noticias y opiniones sobre delitos, creando un espacio para el debate público, pero también para la polarización y la desinformación; 2. El impacto en el sistema legal, donde la presión pública a través de las redes sociales puede influir en la percepción de la aplicación de la justicia y en la demanda de respuestas más rápidas y severas del sistema penal; 3. Los riesgos de la desinformación y la vigilancia, ya que la naturaleza no regulada de las redes sociales puede llevar a la difusión de información errónea y afectar a la imparcialidad del proceso legal.

Por otro lado, en este artículo se debaten tres ideas clave. En primer lugar, la influencia amplificada, referida a la amplificación del impacto de los delitos, lo que lleva a una mayor conciencia pública, pero también a reacciones emocionales intensas. En segundo lugar, el rol activo de los ciudadanos, donde estos son el principal sujeto en la conversación sobre el crimen y cuestionando la narrativa de los medios tradicionales y de las instituciones. Y, en tercer lugar, la necesidad de un análisis crítico de las narrativas del crimen que circulan en las redes sociales debido al riesgo de manipulación y desinformación.

Por último, nos quedaría conocer el impacto real de las redes sociales en la legislación y el sistema penal, la evolución temporal de la reacción social y explorar cómo las percepciones han cambiado o van a cambiar y el estudio entre países para conocer si la reacción social en redes sociales varía en diferentes contextos culturales, políticos o socioeconómicos.

También tiene cabida en este número especial el análisis de Fernández Castejón y colegas sobre la "gamblificación" de los videojuegos (2025). En este fenómeno se introducen mecánicas de juegos de azar, como los *loot boxes* en los videojuegos, y ahí es donde nace el interés criminológico por la preocupación de la exposición de los jugadores, especialmente los menores de edad, a riesgos asociados al juego patológico. Este estudio se basa en el análisis de 50 juegos móviles (los más descargados en la Play Store de España), donde el primer hallazgo es que la mayoría de los videojuegos utilizan micropagos como modelo de monetización, en concreto, el 86% ofrece algún tipo de microtransacción, el

33% incluye *loot boxes* y el 50% presenta avisos de compras dentro del juego. Con estos hallazgos los autores indican que la industria del videojuego es un sector en auge y que genera enormes beneficios, sin embargo, la inclusión de las dinámicas de los juegos de azar (como los *loot boxes*) puede tener efectos perjudiciales para la salud mental de los jugadores, especialmente en menores.

También se mencionan iniciativas a nivel español y europeo a raíz de la preocupación por la protección de los menores. En esta regulación se busca que los proveedores de servicios digitales dirigidos a los menores expliquen de manera sencilla las condiciones de uso de los juegos, las compras dentro del juego y los riesgos para la salud de los participantes. En resumen, el artículo propone la necesidad de regular estas prácticas de juegos de azar en los videojuegos y también nos abre a la reflexión sobre la investigación futura en la que se pueda conocer el impacto real de estas prácticas en la adicción a los videojuegos y, como parte aplicada, conocer mejor los mecanismos preventivos de estos riesgos para los menores.

El último de los artículos de este número especial presenta una revisión de sentencias judiciales en España sobre delitos de odio cometidos en línea entre 2018 y 2022. El objetivo que persigue García Domínguez es analizar las características de estos delitos, el perfil de víctimas y autores y la aplicación del artículo 510 del Código Penal Español (García Domínguez, 2025). La muestra del estudio se compone de 29 sentencias de la base de datos del Centro de Documentación Judicial (CENDOJ).

En primer lugar, en esta muestra se identifica un aumento del número de sentencias relacionadas con delitos de odio en línea durante el periodo de estudio recogidas en CENDOJ, lo que puede indicar un aumento también de sentencias a nivel general de esta tipología. Respecto a los hechos, los delitos de odio en línea son una actividad continuada que se produce durante meses e incluso años y que ocurren de manera exclusiva en el ámbito online. La plataforma Facebook es la más utilizada, seguida de X (antigua Twitter). En cuanto a las víctimas, predominan los colectivos más que las individuales, y cuando son individuales, las víctimas suelen ser hombres y sin relación con el agresor. El perfil de los agresores es un hombre de nacionalidad española, alrededor de 30 años (aunque se destaca que hay un número importante de menores) y con denuncias previas. Las motivaciones discriminatorias se centran en motivos racistas, religiosos, ideológicos y relacionadas con la identidad/orientación sexual. Además, los agresores culpan a las víctimas de los problemas sociales actuales. Los autores utilizan sobre todo los mensajes intimidatorios que crean en las víctimas sentimientos de humillación y afectación de su bienestar, por lo que tienen un impacto emocional importante. En cuanto a los resultados de los procesos, las sentencias en la mayor parte son condenatorias, pero la retirada del contenido solo se ordena en un tercio de los casos. Cuando intervienen circunstancias modificativas se trata de circunstancias modificativas de la responsabilidad penal relacionadas con la reparación del daño y las dilaciones indebidas. Las absoluciones que se producen están relacionadas con la eximente por alteración psíquica del autor, la escasa entidad de la conducta o la falta de motivación discriminatoria del delito, por lo que la aplicación del artículo 510 del Código Penal solo se deja para los casos más graves.

Por último, cabe destacar una serie de implicaciones preventivas: la necesidad de desarrollar técnicas para identificar incitaciones al odio en etapas tempranas, focalizar la prevención en autores recurrentes (sobre todo jóvenes), dirigir acciones de vigilancia de redes sociales, analizar las

razones por las que los tribunales no ordenan retirar contenido, combatir la infradenuncia y fomentar la reparación de las víctimas debido a su alto impacto emocional en estas.

Referencias

Agustina, J. R., Gámez-Guadix, M., & Montiel Juan, I. (2020). *Cibercriminología y victimización online*. Síntesis. http://www.dykinson.com/libros/cibercriminologia-y-victimizacion-online/9788491714545/

Cerezo Domínguez, A., & García Cornejo, R. (2025). Cyberstalking en parejas juveniles. R*evista Española De Investigación Criminológica*, *22*(2), e883. https://doi.org/10.46381/reic.v22i2.883

Convention on Cybercrime (Budapest Convention, ETS No. 185), November 23, 2001. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Díaz Ortega, N., Aguerri, J.C., & Miró-Llinares, F. (2025). ¿Qué estamos haciendo ante las redes sociales? Una revisión sistemática sobre las redes sociales como contexto para la reacción social al delito. *Revista Española de Investigación Criminológica*, 22(2), e881.

Erades Pérez, N., & Sitges Maciá, E. (2025). Perfil de conducta digital, ciberdelitos y cifra negra: análisis de una muestra española. *Revista Española de Investigación Criminológica, 22*(2), e887. https://doi.org/10.46381/reic.v22i2.887

Fernández Castejón, E.B., Aguerri, J.C., & Sampayo Sande, S. (2025). La gamblificación del ocio digital: Análisis de los mecanismos de monetización de los juegos móviles más populares en España. *Revista Española de Investigación Criminológica, 22*(2), e893.

Figueiredo Alves Silva, B., & Miro-Llinares, F. (2024). Vida digital y tendencias delictivas en el sur global: Sobre el impacto del mayor uso de Internet en las oportunidades para la delincuencia. *Revista Española de Investigación Criminológica*, *22*(2), e863. https://doi.org/10.46381/reic.v22i2.863

García Domínguez, I. (2025). Delitos de odio online en España. Una revisión sistemática de sentencias (años 2018-2022). Revista Española de Investigación Criminológica, 22(2), e890.

González García, A., & Campoy Torrente, P. (2018). Ciberacoso y cyberbullying: Diferenciación en función de los precipitadores situacionales. *Revista Española de Investigación Criminológica*, *16*, 1-31. https://doi.org/10.46381/reic.v16i0.149

Grabosky, P. N. (2001). Virtual Criminality: Old Wine in New Bottles?: *Social & Legal Studies*. https://doi.org/10.1177/a017405

Grijalva Eternod, A. E. (2023). Violencia familiar y victimización fuera del hogar en adolescentes. Diferencias de género en relación con la polivictimización. *Revista Española de Investigación Criminológica*, *20*(2), Article 2. https://doi.org/10.46381/reic.v20i2.693

Jordá, C., Píriz, C., & Giménez-Salinas, A. (2024). Los criptomercados ilícitos de tráfico de drogas en la Dark Web: Un estudio exploratorio empírico. *Revista Española de Investigación Criminológica*, *22*(2), Article 2. https://doi.org/10.46381/reic.v22i2.884

Kemp, S. (2024). *Las Ciberestafas: Tendencias, Infractores, Víctimas y Prevención*. Atelier. https://atelierlibrosjuridicos.com/libreria-juridica/las-ciberestafas-tendencias-infractores-victimas-y-prevencion/

Loader, B. D., & Thomas, D. (2000). *Cybercrime: Law enforcement, security and surveillance in the information age*. Routledge.

Lusthaus, J. (2024). Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime? *Annual Review of Law and Social Science*, *20*(Volume 20, 2024), 369-385. https://doi.org/10.1146/annurev-lawsocsci-041822-044042

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence* (Home Office Research Report 75 Research Report 75; Home Office Research Report 75). Home Office. https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

Miró Llinares, F. (2012). *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons. http://www.atelierlibros.es/libros/el-cibercrimen-fenomenologia-y-criminologia-de-la-delincuencia-en-el-ciberespacio/9788415664185

Miró Llinares, F. (2013). La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. *Revista Española de Investigación Criminológica*, *11*, 1-35. https://doi.org/10.46381/reic.v11i0.77

Moreno-Ruiz, D., Montero Montero, D., Romero-Abrio, A., & Musitu-Ochoa, G. (2024). Artículo Roles involved in school violence: Links with the problematic use of social networking sites, self-esteem, and loneliness in adolescents. *Revista Española de Investigación Criminológica*, *22*(1), Article 1. https://doi.org/10.46381/reic.v22i1.900

Pascual, A., Giménez-Salinas, A., & Igual Garrido, C. (2017). Propuesta de una Clasificación española sobre imágenes de pornografía infantil. *Revista Española de Investigación Criminológica*, *15*, 1-27. https://doi.org/10.46381/reic.v15i0.103

Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023PC0366

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065

Rodríguez Ferrández, S., Fernández Castejón, E. B., & Bautista Ortuño, R. (2017). Prevención de la cibervictimización en menores de la provincia de Alicante. *Revista Española de Investigación Criminológica*, *15*, 1-25. https://doi.org/10.46381/reic.v15i0.104

United Nations Office on Drugs and Crime. (2013). *Comprehensive Study on Cybercrime—Draft February 2013*. United Nations Office on Drugs and Crime. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Villacampa, C., & Pujols, A. (2017). Prevalencia y dinámica de la victimización por stalking en población universitaria. *Revista Española de Investigación Criminológica*, *15*, 1-27. https://doi.org/10.46381/reic.v15i0.106

Wall, D. (1999). Cybercrimes: New Wine, No Bottles? En P. Davies, P. Francis, & V. Jupp (Ed.), *Invisible Crimes: Their Victims and their Regulation* (p. 105-139). Palgrave Macmillan UK. https://doi.org/10.1007/978-1-349-27641-7_5

Wall, D. (2001). *Crime and the Internet*. Routledge, Taylor & Francis Group. https://www.routledge.com/Crime-and-the-Internet/Wall/p/book/9780415244299

Yar, M., & Steinmetz, K. F. (2023). *Cybercrime and Society*.