

Siglo XXI: nuevas formas de delincuencia

XXI^e siècle: de nouvelles formes de criminalité

The twenty-first century: new forms of crime

Gizaldi hogeï-bat: forma berriak krimenarena

María de las Nieves NAVARRO-MOZO*

Universidad Europea Miguel de Cervantes

Clio & Crimen, n.º 23 (2026), pp. 473-505

Resumen: El momento presente trae nuevas modalidades de delitos amparados en el mundo cibernético, que se ha convertido en el medio ideal para cometer acciones ilícitas y antijurídicas, así como para que oculte su culpabilidad quien las perpetra. Con el auge de las tecnologías de la información y de la comunicación o TICs, el incremento de delitos y la aparición de otros no parecen tener fin. El número de víctimas es incommensurable, y a esto se añade que el escenario se aprovecha del oscurantismo que representa la red, siendo difícil la reconstrucción de los hechos y la localización del culpable.

Palabras clave: Cibernético. Delito. Oculto. Culpable.

Résumé : Le moment actuel apporte nouvelles infractions protégé par internet, et c'est le lieu idéal pour commettre des actes illégaux et pour qu'il délinquant se cache. Avec l'augmentation des technologies de l'information et de la communication ou TICs, la recrudescence de la criminalité et d'autres délits n'ont pas l'air de se terminer. Le nombre de victimes est énorme, et en plus la scène est sombre sur internet, et reconstituer les événements et localiser du coupable est difficile.

Mots-clés : Cybernétique. Délit. Caché. Coupable.

Abstract: The present momento gets new ways of crimes protect in the cyber world, this one is the ideal place to commit illegal and illicit actions, as well as for hiding the guilty author. From the increase of technologies of information and communication or ICTs, the crimes grow and emerge other without end. The number of victims is enormous, and then the scenary through internet is dark, so it is difficult the reconstruction of facts and location of the criminal.

Keywords: Cyber. Crime Legal. Hidden. Guilty.

Laburpena: Delitu berriak daude gaur egun interneten barira, ekitaldi hauetarako euskarri aproposa delako, erruduna ezkutatu abal izateko ere. IKT-ekin delituak ugaritu egin dira eta veste berri batuk agertu dira. Biktimak banditu egin dira, internetek iluntasuna dakar, beraz gertaerak berreraikitzea zaila da edo erruduna aurkitu.

Giltza-hitzak: Zibeer. Delitua. Izkutuan. Errudun.

* **Correspondencia a / Corresponding author:** María de las Nieves Navarro Mozo. Universidad Europea Miguel de Cervantes. Facultad de Ciencias Sociales. Calle del Padre Julio Chevalier, n.º 2 (47012 Valladolid). – nnavarro@uemc.es – <https://orcid.org/0000-0002-4635-2584>

Cómo citar / How to cite: Navarro Mozo, María de las Nieves (2026). «Siglo xxi: nuevas formas de delincuencia», *Clio & Crimen*, 23, 473-505. (<https://doi.org/10.1387/clio-crimen.28881>).

Recibido/Received: 2026-04-23; Aceptado/Accepted: 2026-05-21.

ISSN 1698-4374 / eISSN 2792-8497 / © 2026 UPV/EHU Press



Esta obra está bajo una Licencia

Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional

1. Introducción

La palabra ciberdelincuencia, supone la comisión de hechos delictivos mediante las nuevas tecnologías, es decir, a través de la red, del universo web que es ilimitado, pues al contrario que los delitos digamos presenciales, que tienen cortapisas físicas como pueden ser por ejemplo los límites fronterizos de un país, sin embargo, el espacio cibernético solamente tiene obstáculos virtuales, que son sorteados por los ciberdelincuentes¹.

Y los actos delictivos tienen múltiples sujetos pasivos, desde personas físicas a personas jurídicas, a más a más, los propios gobiernos de las naciones, y por tanto esto se ha convertido en un grave escollo tanto para la seguridad personal como para la seguridad nacional e internacional, dado que hay actividades criminógenas que pueden llegar a constituir casos de terrorismo informático.

Así como variadas son las víctimas de esta modalidad delictiva, también son heterogéneas las acciones criminales, que socavan el pacífico y natural modo de vida de cualquier pueblo.

En referencia a la parte actora, el sujeto que idea, participa o perpetra estas operaciones delictivas, puede ser alguien que opera de forma individual sin una organización que le sustente, o puede ser algo más complejo desde un punto de vista estructural, al tratarse de un grupo organizado que, yendo más lejos, esté apoyado por un determinado país.

Las razones que impulsan a cometer estos actos, con independencia de causar un mal, que es el móvil último de cualquier delito, pueden ser desde motivaciones de tipo sexual, y sirva como ejemplo el delito denominado *sexting*, hasta fraudes económicos, como son los delitos de ingeniería social, o llegar a desestabilizar el orden internacional, con acciones de calado como el ciberespionaje.

Ante esta situación, parece que la salida más razonable es poner algún límite al crecimiento tecnológico, pero verdaderamente la tan manida expresión de cómo poner puertas al campo se ajusta a esta realidad. La tecnología empleada como pasatiempo puede estar cerca también del ámbito delictivo, creando todo un contexto que llega a tocar lo disruptivo, donde en ocasiones se invierten y solapan los papeles de víctima y victimario²

2. Antecedentes

Si se busca en la historia moderna del crimen, hay que referirse a ataques cibernéticos que poco o nada tienen que ver con el momento presente, pues tienen

¹ Carlos M.^a Romeo Casabona *De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal* (Salamanca: Universidad de Salamanca, 2006), 1-43.

² Miriam Herrera Moreno (dir.) y Beatriz Sánchez Rubio (coord.), *Criminalidad, desviación y riesgo en la ludosfera: Nuevas dinámicas de recreación digital dañina* (Madrid: Dykinson, 2025).

escasa entidad, aunque con consecuencias legales; y así las cosas, hay un personaje como John Thomas Draper, que en los años setenta fue detenido por delinquir en el sistema de compañías telefónicas, de tal forma que creó un sistema a través del cual se podían hacer llamadas gratuitas³.

También está Iam Murphy, Capitan Zap⁴, que actuó en los albores de los ochenta, al introducirse en el sistema de determinada compañía telefónica y variar la hora, por consiguiente, alterando los intervalos del consumo y cambiando las facturas.

Es igualmente en la década de los ochenta, cuando aparecen ataques cibernéticos no conocidos hasta entonces, y que descolocaban a las víctimas de estos sin saber qué estaba pasando, y se trataba de los llamados *ransomware*, que suponían que los ciberdelincuentes retenían archivos de sus víctimas, bajo la amenaza de su publicación o eliminación, si estas últimas no abonaban la cantidad de dinero solicitada para que se les restableciera. Y si *ab initio*, las ofensivas venían siendo más hacia particulares, posteriormente las acometidas se dirigían a su vez hacia empresas, como el conocido gusano *wannacry*, que infectó a miles de ordenadores, inutilizándolos en múltiples empresas de numerosos países⁵.

3. Marcos de ciberseguridad

Para proveer de seguridad al mundo de lo cibernético, se cuenta con estándares de ámbito internacional que ofrecen a las diferentes organizaciones pautas, para gestionar su seguridad, resolver riesgos, y si se da algún incidente conocer cómo gestionarlo, y poder continuar con los negocios.

Es fundamental con vistas a los usuarios de la comunicación e información, donde los ataques e intromisiones a las vías de comunicación se está convirtiendo en algo habitual, que las empresas cuenten con alguna certificación que garantice una adecuada ejecución de los procedimientos en cuanto al tratamiento de datos. Concretamente las normas ISO se componen de estándares que desarrolla y publica la Organización Internacional de Normalización, organización no gubernamental que se fundó en el año 1946, estando su sede social en Suiza, y compuesta por entidades nacionales que la sostienen económicamente junto con la venta de dichas normas. Para la elaboración de estas normas, se cuenta con el conocimiento y colaboración de expertos mundiales divididos en comisiones técnicas. Pero, aunque es-

³ John T. Draper et al., *Beyond The Little Blue Box: The Biographical Adventure of John T. Draper (Aka Captain Crunch). Notorious «phone Phreak», Legendary Internet Pioneer and Ardent Privacy Advocate* (Canadá: Friesen Press, 2018), 30-200.

⁴ Carlos Enrique Álvarez Calderón, *La arquitectura ilícita del ciberespacio: cibercrimen y ecosistemas de la dark web. En C.E. El campo de batalla digital: la defensa nacional en la era algorítmica, Vol. I Infraestructuras de la guerra digital: computación, ciberguerra y defensa del ciberespacio* (Bogotá: ESDEG, 2026), 186.

⁵ Alberto Enrique Nava Garcés. «El caso Wannacry. Ataque en la red», *Revista Penal*, n.º 42 (julio de 2018): 148-164.

tos estándares pueden tener un carácter técnico, también se extienden a otras parcelas como son las de índole social, sanitario, laboral.

Para la ciberseguridad, específicamente está la norma ISO 27032 (cuya predecesora fue la norma ISO 27001 sobre seguridad de la información, con un componente más genérico) denominada «Directrices para la Ciberseguridad», y aporta estándares que protejan la información y comunicación en un mundo global interconectado y digitalizado, dando cobertura a las organizaciones que se mueven en este círculo. Se centra en ciberseguridad de información, redes e internet, y las directrices que proporciona prevén hackeos a través de alertas que reconozcan riesgos en los sistemas, también existen mecanismos de resolución cuando se producen incidentes cibernéticos, e igualmente propone capacitaciones a los integrantes de las entidades que manejen esta norma ISO, y crea un espacio común de colaboración en esta materia⁶.

Con respecto al NIST que depende del Departamento de Comercio de EE.UU., se trata de normas en ciberseguridad, siendo un marco de protección y monitoreo para empresas con la finalidad de que entiendan a qué riesgos se enfrentan en el área digital, que comprendan cómo reducir los ataques, lo que conlleva la protección de la información que manejan y saber enfrentar las dificultades que se presentan. Su creación data del año 1901, y se considera una institución con peso específico en este país, pues el rol que desempeña es potenciar la innovación tecnológica para que el tejido industrial sea competitivo, de tal manera que trabaja en varias áreas, desde desplegar normas de medición para que la ciencia e industria avance con concreción hasta la ampliación de normas que modernicen la calidad de la producción y fomenten la seguridad, para ello entra en colaboración con otras entidades. Asimismo, favorece la investigación en tecnología, gestionando laboratorios de reconocido prestigio internacional en parcelas no sólo tecnológicas; todo esto repercute en su posicionamiento como referente mundial, abordando áreas como la IA, que es otra puerta más hacia un futuro tecnológico.

Sobre lo que une y separa a ISO del NIST, y aunque la comparación entre ISO 27032 y NIST presenta muchas similitudes, sin embargo, la comparativa entre ISO 27001 y NIST podría tener más matices. Con respecto a lo primero, es decir qué las une, daría como resultado que ambas se focalizan en que las diferentes organizaciones sean capaces de identificar y gestionar riesgos, pudiendo implantar los mecanismos de protección que cada cual considere más acertados. Y en cuanto a qué las diferencia, mientras que ISO 27001 se fija en la seguridad de la información, NIST tiene una mayor cobertura pues se dirige a ciberseguridad privada, administración de amenazas, manejo de incidentes y restablecimiento⁷.

⁶ María Camila Arévalo, «ISO 27032, el estándar enfocado en ciberseguridad», *Pirani* (2020): sin paginación.

⁷ Sergio Untiveros, «ISO 27001 vs NIST: un análisis comparativo y su complementariedad», *Aprenda Redes* (noviembre de 2023): sin paginación.

4. Normas internacionales

4.1. Tratado Internacional sobre delitos cibernéticos del 2024, adoptado por la Asamblea General de las Naciones Unidas

En el 2024 fue adoptada la Convención de Naciones Unidas sobre ciberdelincuencia, a la que nos podemos referir como Tratado, y que se aprueba con el objetivo de crear un espacio internacional de legalidad común para la delincuencia cibernética. Esto supone que los países que lo suscriban tilden como delitos determinadas conductas perpetradas a través de las nuevas tecnologías de la información y de la comunicación, y en este marco se encontrarían actos como pornografía infantil y abusos a menores de edad en línea, o estafas en la red, o la utilización ilícita de ciertos dispositivos, o la intromisión en las comunicaciones de forma no legal. También significa que se fortalezcan las acciones coordinadas internacionalmente mediante el trasvase de información para atajar esta problemática, y que se puedan recopilar y transmitir pruebas para algunos delitos debido a su gravedad. Para todo esto se prevé implantar un servicio entre los Estados adheridos que atienda y asesore legalmente⁸.

La UNODC actuó en este caso como una secretaría *ad hoc* para apoyar este proyecto mientras fue negociado. Se considera un importante hito pues todo lo que guarde relación con la comunicación a través de internet está omnipresente, donde el número de víctimas están en constante crecimiento, y como ha quedado patente se deben articular mecanismos nacionales e internacionales en este escenario, que, si no acaban con estas prácticas, al menos pongan coto y den respuesta cuando se cometan, ya que los tentáculos de la ciberdelincuencia son múltiples. Y así la Convención en las Disposiciones Generales de su Capítulo 1, Artículo 1, y sobre sus objetivos, dice que su finalidad es promover las medidas que prevengan y combatan eficazmente la ciberdelincuencia, también fortalecer la cooperación internacional para prevenir y combatir la Ciberdelincuencia, y apoyar la asistencia técnica para combatir la ciberdelincuencia sobre todo en los países en desarrollo.

4.2. Convenio de Budapest sobre ciberdelincuencia, de 23 de noviembre del 2001

Es considerado como el primer acuerdo internacional para delitos cibernéticos, y con esta regulación se fija un marco normativo internacional para afrontar los peligros que entrañan los delitos informáticos, proporcionando legislación penal y sistemas de actuación comunes a los países adheridos al mismo, que sean miembros del Consejo de Europa, y otros países que lo suscriban, basados en la cooperación transnacional en la batalla contra el cibercrimen globalizado.

⁸ Adolfo Athié Cervantes *et al.* «Aprobación del Primer Tratado Internacional en Materia de Cibercrimen», *NOTI BASHAM* (enero de 2025): sin paginación.

Los delitos que se tratan de combatir, están recogidos en el Capítulo II (Medidas que deberán adoptarse a nivel nacional), Sección 1 (Derecho penal sustantivo): El título 1 se refiere a delitos que afecten a la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos (acceso ilícito, interceptación ilícita, ataques a la integridad de los datos y de los sistemas, abuso de los dispositivos), el título 2 recoge los delitos informáticos (fraude y falsificación informática), y los títulos 3 y 4 contemplan los delitos por su contenido (delitos de pornografía infantil, delitos que atenten a la propiedad intelectual y derechos afines).

Coexistiendo ambas regulaciones, Convenio de Budapest y Convención de la ONU, y siendo las dos de carácter internacional, de su lectura se hallan algunas diferencias, como que el Convenio se estableció por el Consejo de Europa y no así la Convención, o que el Convenio busca sancionar hechos delictivos concretos mientras que la Convención presenta un enfoque más general. Ahora bien, como aspecto coincidente, está que las dos normas tienen el mismo fin, como es la lucha contra los delitos cibernéticos.

5. Normativa europea

Además de lo expuesto en anteriores apartados, está la Directiva (UE) 2022/2555, de 14 de diciembre del 2022, sobre ciberseguridad, cuyo contenido es aceptado por los países miembros de la Unión Europea. Asimismo, entrega medios legales que alienten la ciberseguridad en el contexto de la Unión Europea, y proporciona la capacidad de adaptación para las infraestructuras críticas y para los servicios digitales.

Como ha quedado explicado, la Directiva (UE) 2016/1148 nació con el objetivo de desarrollar las capacidades de ciberseguridad de la Unión Europea, y minimizar las amenazas de las redes y de los sistemas de información que prestaban servicios esenciales en sectores fundamentales, así como también fue garantizar el funcionamiento de estos servicios en caso de amenazas, de forma que la economía y la sociedad de la Unión quedaran salvaguardadas. Su derogación se fraguó por estar anticuada y no dar respuesta a los nuevos retos nacionales y transfronterizos, y entre éstos están:

- Engrandecer el espacio de alcance que cubriera sectores económicos y sociales importantes, y por tanto la Directiva (UE) 2022/2555 busca vencer los defectos en relación con la diferencia entre operadores de servicios esenciales y proveedores de servicios digitales.
- La Directiva (UE) 2022/2555, pretende terminar con diferencias entre Estados miembros frente a ciberamenazas, pues podría repercutir en todos los Estados integrantes, y busca superarlo estableciendo unas normas mínimas obligatorias para que se coopere coordinadamente, e igualmente actualizar qué sectores y qué actividades deben cumplir los compromisos sobre ciberseguridad.

- Aun cuando la Directiva (UE) 2022/2555 deje fuera de su campo de acción a las entidades de la Administración Pública, cuyas actividades se desarrollen dentro de la seguridad nacional, así como garantizar el cumplimiento de la legalidad, sin embargo, aunque la relación de estas entidades con estas áreas sea residual, sí que estarían incluidas en la aplicación de esta Directiva.
- Otro más, es que las entidades que estén incluidas en el ámbito de aplicación de la Directiva (UE) 2022/2555, se clasifican en dos para determinar su grado de cumplimiento sobre cómo tienen que gestionar los riesgos en ciberseguridad, y esa división es en entidades esenciales y entidades importantes, en función del mayor o menor grado de criticidad, en función del servicio que den o en función del tamaño que tengan.
- La Directiva (UE) 2022/2555 sobre el ya mencionado equipo de respuesta a incidentes de seguridad CSIRT, hace hincapié en que, al manejar datos importantes, debe controlarse por los Estados miembros que este organismo cuente con la infraestructura adecuada para tratar dicha información.
- En cuanto a la IA, la Directiva (UE) 2022/2555, recoge que estaría encuadrada dentro de la tecnología innovadora que debe ser fortalecida, si ello sirve para prevenir y detectar mejor los ciberataques.
- La Directiva (UE) 2022/2555 contempla cómo la Agencia de la Unión Europea para la ciberseguridad (ENISA), la Comisión y los Estados miembros, deben procurar seguir un camino paralelo al del resto de normas internacionales.
- Esta Directiva (UE) 2022/2555 mantiene el respeto a los derechos fundamentales, como el derecho a la vida privada y a las comunicaciones, el derecho a la protección de datos personales, el derecho a la presunción de inocencia o el derecho a la tutela judicial efectiva.
- La IA es objeto de tratamiento en el Reglamento (UE) 2024/1689, de 13 de junio, del Parlamento Europeo y del Consejo, cuyo objetivo es que se haga buen uso de la IA de acuerdo con lo imperante en el ámbito geopolítico de la Unión, y que se proteja lo recogido en la Carta de Derechos Fundamentales de la Unión Europea, a la vez que se eviten limitaciones a la utilización de IA salvo las que pudiera imponer esta norma. Esta regulación es de aplicación progresiva, cuya implantación definitiva será en agosto del 2027, para que dé tiempo a que las empresas puedan amoldarse a la misma. En este Reglamento se fija un orden de prelación en cuanto a formas de IA en base al nivel de riesgo, y así nos encontramos desde sistemas que conllevan un riesgo real para la seguridad o los derechos fundamentales y por consiguiente estarían vetados, hasta sistemas con poco o nulo riesgo y que no conllevarían ninguna exigencia añadida, pasando por sistemas de alto riesgo que necesiten controles rigurosos, u otros sistemas de poco riesgo que precisen ciertas condiciones que aporten transparencia a los consumidores⁹.

⁹ Ana M.^a Ruanova Aranaz, «Regulación de la Inteligencia Artificial: Europa abre el camino», *Abogacía de Valladolid – Revista semestral del Ilustre Colegio de la Abogacía de Valladolid* (2025): 38-39.

6. Regulación legal nacional

Además de la normativa vista, a continuación, se refieren las siguientes leyes:

6.1. Ley 13/2015, de 5 de octubre, de reforma de la Ley de Enjuiciamiento Criminal

Esta reforma introduce cambios, concretamente se actualiza en la utilización de las TICs con la finalidad de cometer hechos delictivos. Esas modificaciones están previstas en los siguientes preceptos:

- Libro II (Del sumario), Título VIII (De las medidas de investigación limitativas de los derechos reconocidos en el Artículo 18-1 de la Constitución —en este precepto se reconoce el derecho al honor, intimidad personal y familiar y a la propia imagen, garantizándose en su apartado 3 el secreto de las comunicaciones, y en su apartado 4 se establece la limitación del uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos—), Capítulo V (La interceptación de las comunicaciones telefónicas y telemáticas —Artículo 588 *ter*—), Capítulo VI (Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos —Artículo 588 *quater*—), Capítulo VII (Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización —Artículo 588 *quinquies*—), Capítulo VIII (Registro de dispositivos de almacenamiento masivo de información —Artículo 588 *sexies*—), Capítulo IX (Registros remotos sobre equipos informáticos —Artículo 588 *septies*—).

Estas normas recogen poder intervenir comunicaciones telefónicas y telemáticas para investigar delitos como terrorismo, delitos dolosos castigados con pena con límite máximo de al menos tres años de prisión, y aquellos cometidos dentro de organización criminal, y para delitos que se cometan por medio de instrumentos informáticos o con uso de tecnología de la información y comunicación.

6.2. Real Decreto 43/2021, de 26 de enero

Hubo una Directiva (UE) del Parlamento Europeo y del Consejo de 6 de julio del 2016, la 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, que es conocida como la Directiva NIS, y su traslación al sistema legal en España se realizó con el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad en las redes y sistemas de información. Esta norma va dirigida a regular la seguridad en redes y sistemas de información empleados en servicios esenciales y digitales, y por consiguiente que haya un avance en la protección para hacer frente a los riesgos existentes, toda vez que para acometer esto se establece un marco de colaboración

a nivel nacional y con países de nuestro entorno de la Unión Europea. Todo ello se materializa mediante acciones, como designar autoridades competentes en el ámbito de seguridad en redes y sistemas de información; o también sobre el punto común de contacto se desarrollan sus funciones de enlace, que permitan la colaboración entre Estados miembros de la Unión Europea y con el grupo CSIRT, que es un equipo de respuesta a aquellos incidentes que sobre seguridad se puedan producir en computadoras.

Con posterioridad, el Real Decreto-Ley 43/2021, desarrolla el anteriormente citado RDL 12/2018, de 7 de septiembre, con relación al marco de seguridad tanto en redes como en sistemas de información e igualmente para la supervisión de que se cumplan las obligaciones que en el terreno de seguridad tienen los operadores de servicios esenciales y los proveedores de servicios digitales, y también con relación a la gestión de los incidentes en seguridad que pudieran producirse. En cuanto a los servicios a los que se aplica este RDL 43/2021, son los servicios esenciales que dependan de redes y sistemas de información comprendidos en sectores estratégicos de los recogidos en el Anexo de la Ley 8/2011, de 28 de abril (como son el sector de la administración, el espacio, la industria nuclear o química, las instalaciones de investigación, las tecnologías de la información y las comunicaciones, etcétera), y asimismo es de aplicación a los servicios digitales que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube; todos ellos dada la importancia de los temas que tratan y porque pueden sufrir amenazas cibernéticas, se debe fijar un escudo de protección que los ampare.

7. Algunos casos de delincuencia cibernética

En el propio contenido de los delitos, hay interrelaciones en gran parte de ellos, y por tanto hay veces que la respuesta legal puede ser coincidente. Con la aparición en el mundo del crimen del uso de medios digitales, hay delitos que ya existían empleando otras técnicas, como los fraudes económico-financieros o la suplantación de identidad y que ahora se siguen por medio de internet, pero hay otros propiamente cibernéticos, como son los de manipulación de sistemas o los ataques DDoS que saturan un servicio.

7.1. Usurpación de identidad digital mediante IA

Tiene la finalidad de causar un mal que puede ser de grandes dimensiones, porque el delincuente se hace pasar por otra persona para la comisión de alguna actividad fraudulenta, como puede ser la adquisición de bienes o servicios.

El sistema de apropiación de datos personales de la víctima en el llamado *phishing*, se hace enviando un correo electrónico que manda un enlace redirigiendo al usuario a una página fraudulenta para así lograr su objetivo. Hay una Sentencia de la Audiencia Nacional de la Sala de lo Penal, la 8/2020, de 15 de sep-

tiembre, que recoge cómo los acusados se unieron para conseguir beneficios monetarios, y lo hacían obteniendo dinero tanto de entidades públicas como de particulares mediante el uso de documentación falsa.

Otra forma de actuación es mediante la creación de un perfil falso utilizando la imagen y nombre de la persona suplantada para que resulte convincente.

Este delito está recogido en el artículo 401 del Código Penal como usurpación del estado civil, cuya sanción puede llegar a pena prisión de hasta tres años.

En este contexto procede hacer una mención especial a la Inteligencia Artificial o IA generativa, siendo ésta una herramienta que se puede emplear con fines de ciberseguridad, pero que tiene como contrapartida su uso también para la comisión de ciberdelitos, como *v.gr.* los ataques encuadrados en este delito de *phishing*.

El famoso *Chat GPT* y la IA generativa, son herramientas que los ciberdelincuentes pueden usar para cometer sus estafas y demás, pues son relativamente sencillas, y con ellas se pueden imitar imágenes y voces creando ambientes falsos, generar espacios de comunicación ficticios, páginas *checkout* engañosas, igualmente se podrían crear sitios web fraudulentos, imitando a una página web que parezca veraz, consiguiendo información del usuario en cuestión, también se pueden crear documentos de identidad falaces por medio de algún software ilegal que se encuentran en la Dark Web (como el llamado *Worm GPT* con los que se pueden robar datos)¹⁰.

La Unión Europea ha creado un marco legal para la revolución que supone la llegada de la IA, y lo ha consolidado con la aprobación del Reglamento (UE) 2024/1689, de 13 de junio *supra dictus*, pretendiendo no sólo normativizar esta realidad tecnológica, sino que ello se haga sin olvidar el bien de la colectividad y el respeto a la dignidad con una concepción ética y humanista. En la mencionada IA generativa como el *Chat GPT*, viene establecido que se tendrán que desvelar los contenidos creados con IA, así como mantener el respeto a derechos de autor, evitando ilegalidades. Esta norma, aunque fija mecanismos de control, no pretende cercenar el avance tecnológico del tejido empresarial por lo que incluye mecanismos que las favorezcan, y así se pueden nombrar las llamadas *softlaw* o normas de cumplimiento voluntario, cuyo uso es potenciado por este Reglamento, y que se pueden definir como códigos de buen comportamiento en el empleo de la IA cuya confección puede recaer en proveedores.

7.2. Espionaje en las redes

Ciberspionaje *vs* espionaje tradicional, y es que mucho han cambiado los tiempos desde las pinchadas de teléfonos sin autorización judicial para obtener informa-

¹⁰ Alfonso Cervera, «Todo lo que necesitas saber sobre WormGPT», *Recoverit* (mayo de 2026): sin paginación.

ciones. En los momentos actuales, este sistema se da en las redes informáticas, en el ciberespacio, y no sólo se interceptan mensajes o se recaban datos sensibles, sino que cabe su manipulación o destrucción¹¹.

Éste es un término amplísimo que incluye la sustracción de contraseñas, cuentas bancarias, conexión a equipos informáticos de terceros, y otros más, siempre sin el permiso del titular de esa información y con la finalidad de ocasionar daños y perjuicios a esa persona o entidad. En definitiva, se trata de conseguir datos e información de un tercero sin su permiso, y como esto se desarrolla en el ciberespacio, de ahí su nombre. Y es que aun cuando al referirse a ciberespionaje, la mente nos transporta al espionaje entre países que viene afectando al potencial ofensivo y defensivo además de otros aspectos, no se debe dejar de lado que también se puede dar entre empresas y entre particulares, como se ha visto *ut supra* y como se seguirá abordando. El ciberespacio alberga conductas criminales como el terrorismo¹².

En el ciberespionaje se dan múltiples factores, desde que el sistema tecnológico cuente con lagunas de seguridad y por tanto sea vulnerable, hasta disponer de los recursos y conocimientos necesarios para llevar a cabo un ataque cibernético.

El ciberespionaje va dirigido a ámbitos reducidos, cuando se trata de espiar a una persona física, pero esto se amplía teniendo como objetivos a empresas, y avanzando en esa escalada estaría el espionaje entre Estados. En este sentido, las ciberamenazas digitales se convierten en algo verdaderamente peligroso, pues atañe a la seguridad de los países, a las estructuras políticas, a la seguridad internacional, convirtiéndose en ciberterrorismo.

Si se sigue el criterio de los noticieros patrios u otros más, a la cabeza del pelotón podrían estar los Estados Unidos, aunque no tiene patente de corso y por ello hay otros países como son Rusia y China¹³.

Este medio de espionaje y de ciberinteligencia cuando corre a cargo de gobiernos, se puede llevar a efecto *v.gr.* con el conocido DoS, que no hace otra cosa sino denegar un servicio, cortando el normal funcionamiento de los modos de comunicación a los que va conducido su ataque. Otro método que se viene empleando es introducir virus en el sistema objeto de ataque, *haec omnia iam prius sunt perpensa*.

Para poder ejecutar estas acciones, tanto positivas como negativas, habría que hacer una distinción entre el comúnmente conocido *hacker*, cuya acepción es más la de un experto informático que con sus conocimientos técnicos, detecta fallos en

¹¹ Gema Sánchez Medero, «El ciberespionaje», *Derecom-Nueva Época* (2013): 115-124.

¹² Mercedes Suárez de la Torre, «Ciberespionaje: una nueva forma de ataque y de defensa cibernética», *Antenas Neológicas-Red de neología del español* (marzo de 2016): sin paginación.

¹³ Francisco Javier Montilla Aguilera, «El ciberespacio desde la perspectiva china: análisis estratégico y operacional», *RDEN Revista de Estudios Internacionales* (mayo de 2025): sin paginación.

estos sistemas cibernéticos aportando mejoras en su manejo y seguridad. Y en el lado opuesto estarían los *crackers*, que son los que rompen los diques de seguridad informática, vulnerando las protecciones de los sistemas y actuando sin el permiso de los propietarios, ya sea por deseos de notoriedad, de crítica, de provocación, o simplemente crematístico.

En el historial de estas actividades, se ha fijado un antes y un después con la ciber guerra del llamado virus *Stuxnet* del año 2010, se trataba de un gusano informático que atacó las instalaciones nucleares de Irán no solamente a nivel de ordenadores, y su sistema operativo *Windows*, sino también físicamente al *hardware*, saltando de una computadora a otra; la rumorología mundial ubica su creación y ataque en los servicios de inteligencia estadounidenses e israelíes¹⁴.

Al hilo de lo anterior y más recientemente, el grupo «pirata» denominado *Storm-0558*, atacó a Microsoft y a cuentas de correos electrónicos, en parte correspondientes al Departamento de Comercio de los EE. UU., y parece ser que presuntamente este grupo actuante estaba vinculado a China. La situación fue que llevó a cabo un ciberataque y ciberespionaje contra Microsoft aprovechando cierta vulnerabilidad en esta compañía, y de este modo consiguió acceder a correos de organizaciones en Europa y también de empresas privadas, así como del propio estado norteamericano¹⁵. La respuesta de la compañía Microsoft fue bloquear el acceso de los ciberdelincuentes, protegiendo mejor el sistema de seguridad y de claves de acceso. Y es que tal y como se concibe la actual geopolítica, uno de los desafíos que tiene ante sí EE. UU. para su seguridad nacional es precisamente el ciberespionaje, y al igual que pasaba en la guerra fría u otras guerras, el objetivo es conseguir información que otorgue ventajas al país que la obtenga, y en este tablero del *spygame*, EE. UU. tiene un grandísimo competidor como es China¹⁶.

En España, la respuesta legal penal al ciberterrorismo, se encuentra en el Código Penal, en particular el capítulo VII sección segunda se refiere a los delitos de terrorismo, y en el artículo 573-2 habla sobre la consideración de actos terroristas a los delitos informáticos tipificados en los anteriormente analizados artículos 197 *bis*, y 264 a 264 *quater*, cuando los hechos se cometan con alguna de las finalidades contempladas en este artículo 573-1, es decir: subvertir el orden constitucional, desestabilizar a instituciones políticas, económicas o sociales del Estado, u obligar a los poderes públicos a hacer o no hacer algo / alterar la paz / desestabilizar a una organización internacional que sea especialmente crítica con aspectos que propugnan quienes llevan a cabo estos actos / provocar terror en la población, con la salvedad de que algunos de ellos desencadenen mayor pánico debido a la violencia ejercida, o por el número de personas que se puedan ver afectadas.

¹⁴ Guillermo Julián, «Stuxnet: historia del primer arma de la ciber guerra», *Genbeta* (diciembre de 2013): sin paginación.

¹⁵ Kevin Lanier, «Storm-0558 Forensic Analysis», *Cyber* (marzo de 2025): sin paginación.

¹⁶ Kevin P. Newmeyer, «Cyber Espionage: A threat to National Security», *Center for Hemispheric Defense Studies Security and Defense Studies Review An Interdisciplinary Journal*, 10 (2010): 113-122.

Si se pretenden conseguir dichas finalidades, también cabe incluir el artículo 197 *ter*, que contempla como terrorista al que, sin permiso, produzca, adquiera para uso propio o facilite a terceras personas programas informáticos, o contraseñas de ordenador, pudiéndose imponer prisión de hasta dos años.

7.3. Extorsión a través del ciberespacio

Se trata de un delito por el cual el sujeto activo de la acción lleva a cabo acciones amenazantes hacia el sujeto pasivo, y lo hace mediante recursos digitales, de tal forma que busca compeler a la víctima para que realice actos perjudiciales para sí misma o que dañen a otro tercero. Como más adelante se indica, mediante el ciberespacio, éstas se centran en menores de edad o colectivos vulnerables.

El ciberacosador, unas veces reclama una suma de dinero como contrapartida a la no publicación de información privada de la persona acosada, pero en otras ocasiones la motivación no es monetaria, sino que busca coaccionar a la víctima solicitando otras cosas, como practicar sexo o que la víctima le mande fotos, vídeos. Siguiendo con esta línea argumental, cabe subrayar la violencia que a través del ciberespacio sufren las mujeres¹⁷, y es que desde *in illo tempore* las mujeres no han tenido precisamente contextos ventajosos en la mayor parte de las sociedades, y que aun a día de hoy siguen existiendo manifestaciones contra el sexo femenino por el mero hecho de serlo, siendo el entorno digital un terreno propicio, a lo que se suma que en multitud de ocasiones la víctima lo vive de forma silente. Para combatir estos planteamientos, los poderes del Estado deben arbitrar las acciones pertinentes, y ello no es posible sin la ayuda de la sociedad en su conjunto.

Una clase de ciberextorsión es conseguir información privada pero no de carácter sexual, sino datos personales de alguien anónimo tales como la dirección, teléfono, centro de trabajo, que amenaza con revelar y difundir si no se le paga, y a este modelo de extorsión se le llama *doxing*.

En esta línea argumental, hay un caso que ha alcanzado notoriedad desde hace años por la frecuencia en su comisión, la denominada *sextorsión*¹⁸, en la cual la in-

¹⁷ Irene Bajo-Pérez, «Ciberviolencias machistas en Instagram: relación entre el número de seguidores y seguidoras y la violencia recibida», en *Feminismo Digital. Violencia contra las mujeres y brecha sexista en Internet* (Madrid: Dykinson, 2021), 711-730. Juana M.^a Ruiloba-Núñez, «Acciones públicas frente a la violencia de género digital. Un acercamiento comparado desde el nivel autonómico español», en *Feminismo Digital. Violencia contra las mujeres y brecha sexista en internet* (Madrid: Dykinson, 2021), 398-420. Dolores Cidoncha Romero y M.^a Ángeles de la Cruz Fortún, *La violencia sexual y las nuevas tecnologías. Guía para jóvenes y adolescentes* (Zaragoza: Instituto Aragonés de la Mujer Gobierno de Aragón, 2023), 1-71.

¹⁸ Irene Montiel Juan, Enrique J. Carbonell Vayá y Miriam Salom García, «Victimización Infantil Sexual Online: Online Grooming, Cibe rabuso y Ciberacoso Sexual», en *Delitos sexuales contra menores. Abordaje psicológico, jurídico y policial* (Madrid: Tirant lo Blanch, 2014), 223-224. Raquel López Jiménez,

timidación proviene de la posibilidad de divulgar contenido sexual. Para acceder a esa información íntima, no pocas veces el acosador disfraza su personalidad, y a través del ciberespacio en redes sociales se hace con imágenes de la persona a la que va a someter a este tipo de acoso, aunque otras veces puede obtener imágenes sexuales con el consentimiento de la víctima, pero esto último no significa que esté autorizado para difundirlas.

La cobertura y respuesta penal a la *sextorsión*, viene de varios tipos penales, pues como *sextorsión* no hay un tipo penal que así lo contemple. Y a este respecto, se puede enmarcar en delitos como:

- Explotación sexual, que es una actividad delictiva tipificada en los artículos 187 y 188 CP, que refiere el término prostitución y explotación sexual. Es una tipología delictiva que atenta contra la libertad sexual y se establece una diferencia según sean las víctimas mayores o menores de edad. Las penas para imponer en los mayores de edad pueden ser de hasta cinco años, y la casuística contempla el supuesto de que se le obligue a ejercer la prostitución ejerciendo violencia, intimidación o engaño, así como abusando de su vulnerabilidad. Otro supuesto que conlleva penas de hasta cuatro años de prisión, es cuando el explotador se lucra del ejercicio de la prostitución de otra persona, aun cuando esta última consienta en ello porque es vulnerable o porque las condiciones que se imponen a la víctima para que se prostituya son abusivas. A mayores está el caso de los menores de edad que recoge varios supuestos, y que en el tipo básico se establece una pena privativa de libertad de hasta cinco años para quien induzca, promueva la prostitución no sólo a menores sino también a personas con discapacidad necesitadas de especial protección, o si se lucra de ello, y además esta pena se agrava en determinados casos, como cuando la víctima tenga menos de dieciséis años o los hechos se han cometido con violencia.
- Abuso y corrupción de menores de edad, que se interpreta como la captación de menores también de personas con discapacidad que son necesitadas de especial protección, para espectáculos exhibicionistas o de pornografía, ya sean públicos o privados, así como para la creación de material pornográfico con independencia de cuál sea su soporte. Estos actos los incluye el legislador en el artículo 189-1 a) CP y pueden conllevar una pena de prisión que llegue a alcanzar los cinco años.
- Agresión sexual, otro de los delitos en los que podría enmarcarse, recogido en los artículos 178 a 180 CP. Haciendo una breve mención al mismo, cabe

Victimización Sexual y Nuevas Tecnologías: Desafíos Probatorios (Madrid: Dykinson, 2021). Carmen Rodríguez-Domínguez y Mercedes Durán Segura, «Sextorsión: nueva forma de violencia hacia chicas adolescentes», en *Participación, políticas sociales y protección de la infancia: aprendiendo con los niños y las niñas a construir sociedades inclusivas* (Sevilla: CIPI, 2018), 128-136. Rosana Martínez Román, Yolanda Rodríguez Castro y María Lameiras Fernández, «Grooming, sexting y sextorsión, los nuevos fenómenos de ciberviolencia: la coeducación como media de prevención», en *Ensayos Ciberfeministas* (Madrid: Dykinson, 2023), 52-67.

decir que tras la aprobación de la LO 10/2022, de 6 de septiembre de Garantía Integral de la Libertad Sexual, se lleva a cabo una notable reforma en los delitos contra la libertad e indemnidad sexual, y así nos encontramos con la eliminación de la distinción entre abuso sexual y agresión, ya que serán todas agresiones sexuales cuando se atente contra la libertad sexual sin mediar consentimiento. Y lo que más incide en la temática que nos ocupa, es la incorporación de conductas delictivas cuando se efectúan a través de las redes sociales, sirva por caso el *child grooming* (acoso a menores de edad desde internet)¹⁹, pronunciándose el Preámbulo de esta Ley expresamente en este sentido.

Esta misma Ley en su Disposición Final Cuarta, modifica algunos artículos de la LO 10/1995, de 23 de noviembre, del Código Penal, y referente a la cuestión tecnológica, el artículo 183 va a contemplar delitos sexuales (pornográficos, exhibicionismo...), perpetrados contra menores de dieciséis años y a través de internet, teléfono u otra tecnología de la información y comunicación, pudiendo recaer penas de hasta tres años de prisión.

- Tenencia y distribución de pornografía de menores, o cuando hayan sido utilizadas personas con discapacidad necesitadas de especial protección; estos hechos delictivos son contemplados en el artículo 189-1 b) CP, cuya pena de prisión podría ser de hasta cinco años. Y la redacción de este precepto, expresamente habla de «por cualquier medio», por lo que implícitamente también se incluirían medios digitales.
- También podría ser considerado, como un delito de amenazas, que se sitúa en los artículos 169 y ss CP. Al igual que en el párrafo anterior, las amenazas se pueden hacer por escrito, por teléfono o por cualquier medio de comunicación o de reproducción.
- Otros más son los delitos que atentan contra la intimidad del artículo 197 del CP, que ya han sido abordados anteriormente.
- Asimismo, podría constituir un delito de revelación de secretos, ubicado en el artículo 197 CP. Y a este respecto se trae a colación una Circular de la Fiscalía General del Estado, en concreto la 3/2017, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos. Y en su introducción dice que dicha Ley refiere en el Preámbulo y en su apartado XIII, que las modificaciones introducidas en estos tipos de delitos han sido posibles al introducir en el Ordenamiento Jurídico la Directiva Europea 2013/40/UE, que trataba sobre ataques a sistemas de información, e igualmente han sido factibles, porque el legislador ha querido dar cobertura legal a aquellas conductas que impliquen divulgar imágenes o grabaciones de un tercero sin su permiso, y que supon-

¹⁹ Abraham Castro y Eva Carballo, «Cuestiones más significativas de la Ley Orgánica 10/2022, de 6 de septiembre de garantía integral de la libertad sexual», *Legal Today* (octubre de 2022): sin paginación.

gan un atentado a su intimidad. Por tanto, la Directiva 2013/40/UE es el marco jurídico europeo donde se fijan una serie de normas mínimas que tienen como finalidad la prevención y la sanción de delitos informáticos, tales como el acceso ilícito o el sabotaje de datos, e implanta la obligatoriedad para los Estados miembros de tipificar éstas y otras conductas cibernéticas penalmente reprobables.

—O cabe la opción de haber delinquirido al interceptar información personal a través de la red, lo que se acomete en el artículo 197 CP.

Las anteriores figuras delictivas dan respuesta a este tipo de actuaciones de *sextorsión*, y la dan en función del bien jurídico que se quiera proteger porque haya sido conculcado mediante las nuevas tecnologías de la comunicación y de la información, y puede ser desde el derecho a la libertad e indemnidad sexuales hasta el derecho a la intimidad y demás.

Procede traer a colación una Sentencia del Tribunal Supremo del año 2018 (STS 377/2018, de 23 de julio), por la que se condena a un sujeto que tuvo acceso a archivos personales con contenido sexual de la víctima, y logró furtivamente esa información a través de herramientas informáticas. Posteriormente atemorizó de tal manera a esa mujer infundiéndole en ella temor a que difundiera dichas imágenes que pudo obligarla, a lo que ésta accedió, a tener varios contactos con él por medio de un programa de mensajería instantánea, y en estas comunicaciones ella debía desarrollar prácticas sexuales, por lo que él fue condenado por la Audiencia de Valencia como responsable de delitos de abuso sexual, contra la intimidad y de amenazas. La representación del condenado recurrió este fallo en casación ante el Tribunal Supremo, alegando infracción de ley e infracción de precepto constitucional, declarando finalmente dicho Tribunal que no ha lugar al recurso y condenándole en costas.

Al final se hace necesario el trabajo en políticas inclusivas incluso desde los primeros años de la infancia, así como que se involucre más la ciudadanía para lograr una sociedad más armoniosa²⁰.

7.4. Ciberbullying

No se trata de un delito de nueva construcción aquello de hostigar a otra persona, lo que sí entraña son situaciones recurrentes que se producen desde edades tempranas hasta más allá. Y en este caso, el acoso se efectúa a través del medio digital, y en los últimos años ha habido un importante crecimiento con el auge de las redes, por lo que no es anecdótico que esta situación se produzca entre adoles-

²⁰ Antonio Salvador Jiménez Hernández *et al.* *Participación, políticas sociales y protección de la infancia. Aprendiendo con los niños y las niñas a construir sociedades inclusivas* (España: CIPI, 2018), 128-138.

centes y jóvenes en un entorno educativo²¹. Conforme a lo establecido tanto por el Alto Tribunal como la Fiscalía General del Estado sobre el tratamiento del acoso en centros escolares²², se desprende que el *bullying* engloba una serie de comportamientos repetidos en el tiempo y en los que uno o varios alumnos actúan sobre la víctima de tal forma que la provocan miedo, sentimientos de inferioridad y angustia, menoscabando a la víctima tanto física como moralmente.

Este hostigamiento genera tal sensación de ansiedad en la víctima, que puede desembocar en acciones autolíticas en los casos más dramáticos. Caso famoso fue el de la joven canadiense Amanda Todd²³ que se suicidó en el año 2012 después de colgar 1 mes antes un vídeo titulado «Mi historia: Agobio, Acoso, Suicidio y Autolesiones» en el que relata sus experiencias. Su historia empieza cuando mediante engaños y a través de una webcam enseña su pecho, y posteriormente se la pide hacer un *striptease* online bajo amenaza de que, si no accede, el agresor publicaría su *topless*. El delincuente cumple su amenaza enviando su foto con el torso descubierto a amigos, conocidos, profesores, etcétera, y después de traslados de centros de estudios y numerosas penalidades a causa de esto, el desenlace es que un día toma la decisión de quitarse la vida.

Hay numerosas sentencias sobre esta cuestión, sirva como ejemplo la SAP Málaga 452/2009 de 16 de septiembre, siendo ponente Julio Manuel Ruiz-Rico Ruiz-Morón, y considerándose un delito contra la integridad moral y delito de lesiones, de cuyo contenido aparece acreditado cómo tres menores agreden a otra menor y lo graban para después difundirlo; se condena entre otros por lesiones psíquicas del art. 147 CP, por un delito contra la integridad moral del art. 173-1 CP, por un delito de encubrimiento y revelación de secretos del art. 197 CP, y en el caso de la responsabilidad civil recae en las victimarias y sus padres.

7.5. Crimen e Inteligencia Artificial

La IA está de plena actualidad, aunque no es algo del todo novedoso, pero en estos momentos se ha popularizado con la eclosión de la IA generativa del ya famoso *Chat GPT* que cualquier adolescente maneja y que lanzó la empresa estadounidense *Open AI* en el año 2022.

²¹ Orietta Mireya Neyra Castilla (2021), «Ciberbullying: El acoso escolar en el ciberespacio e implicancias psicológicas», *Hamut'ay*, 8, n°1 (2021): 67-74.

²² STS 1218/2004, de 2 de noviembre, siendo ponente el Excmo Sr. D. Juan Ramón Berdugo Gómez de la Torre. Se establece que la integridad moral es un concepto propio y un valor de la vida humana pero independiente del derecho a la vida, a la integridad física, a la libertad y al honor.

STS 819/2002, de 8 de mayo, siendo ponente el Excmo Sr. D. Julián Sánchez Melgar, en la que también se determina el delito contra la integridad moral.

Instrucción 10/05 de la Fiscalía General del Estado, sobre el tratamiento del acoso escolar desde el sistema de justicia juvenil, que refiere que acoso escolar o el término anglosajón de *bullying* siempre ha existido entre iguales menores.

²³ Gobierno de Canarias, <https://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/producto/el-caso-de-amanda-todd-subtitulado/>

Pero más allá de su uso cotidiano en el sistema educativo, la IA es una potente herramienta para otros campos como la medicina e incluso la minería, etcétera. Y como cabría esperar, también para el mundo del hampa.

Su uso en el crimen transnacional²⁴ es un hecho, como asimismo lo es que sirve para potenciar delitos ya existentes y para crear otros nuevos. Y se debe garantizar que se realice con transparencia e imparcialidad.

Con la IA se pueden manejar ingentes cantidades de datos en lapsos temporales cortos, de forma que el crimen organizado allende las fronteras, gana en operatividad, sofisticación y ocultación a los ojos de las Fuerzas y Cuerpos de Seguridad de cualquier Estado, ya que descubrir su trazabilidad pasa a ser una misión muy compleja, pues los algoritmos en que se basa no siempre se llegan a conocer, debido entre otros motivos a que la propia IA puede llegar a producir algunos algoritmos, pues tiene un sistema de aprendizaje automático.

Estas organizaciones internacionales criminales cuentan con tecnología, infraestructura, plataformas de mensajería cifrada —véase el caso de Pável Dúrov como CEO de *Telegram* que ha tenido problemas con la justicia, porque se sospecha que el uso de esta plataforma es para llevar a cabo actividades turbias por los delincuentes—, con el uso de criptomonedas que puede llegar a ser otra herramienta al servicio de la delincuencia, igualmente con la diversificación de las inversiones en paraísos fiscales, generando todo un entramado empresarial dirigido a confundir al controlador.

Mediante la IA se pueda atajar el crimen²⁵, previendo conductas, analizando información, y que ello se haga bajo el paraguas de la transparencia e imparcialidad y evitando que se conculquen derechos fundamentales, y es que la IA en sí misma no es algo negativo, sin embargo, sí lo es si las manos en las que cae son delincuentes.

Aun cuando la utilización de esta tecnología tiene como máximos exponentes a EEUU y al gigante asiático China, sin embargo la generalización mundial de su uso hace que se haya extendido por todos los rincones del planeta con mayor o menor acierto, y concretamente en España las compañías no se muestran indiferentes al avance tecnológico, de tal manera que las grandes empresas abanderan el uso de esta tecnología, seguido por medianas empresas, pequeñas empresas y finalmente microempresas, véanse los porcentajes en la subsiguiente gráfica referidos al año 2024:

Empresas grandes	Empresas medianas	Empresas pequeñas	Microempresas
44%	20,6%	8,6%	7%

²⁴ María Guadalupe Valenzo Salgado, «Inteligencia Artificial como instrumento del crimen organizado transnacional», *Ibero-Ciencias Revista Científica y Académica*, n.º especial UAGro (junio de 2026): 1-16.

²⁵ Aldo Fernando Rejas de la Peña *et al.* «La Inteligencia Artificial en la lucha contra el crimen organizado», *Ciencia Latina*, n.º 4 (2024): 2144-2158.

En cuanto a la categoría de necesidades u objetivos a cubrir por esta tecnología de IA en el año 2024, están las siguientes:

Empresas de 10 o más personas empleadas	Microempresas	Total empresas
Análisis de lenguaje escrito 44,7%	Realizar análisis del lenguaje escrito 51,3%	Tecnología más usada es realizar análisis de lenguaje escrito
Automatizar flujos de trabajo o ayudar a tomar decisiones 39%	Convertir lenguaje hablado en formato legible (reconocimiento de voz) 40,6%	También crece el porcentaje en el uso del aprendizaje automático
Generar lenguaje escrito o hablado 37,8%	Analizar lenguaje escrito, aprendizaje automático también ha crecido en el 2024	En menor posición están las tecnologías que convierten el lenguaje hablado en formato legible por máquina

Fuente: tablas de elaboración propia, información sacada el Gobierno de España²⁶.

7.6. Stalking

Otra modalidad de ciberdelito es el *stalking*, es decir lo que se entiende como acoso u hostigamiento, una conducta típica y antijurídica, cuyo *modus operandi* consiste en el deseo de controlar de manera obsesiva a otra persona, que se ha propagado rápidamente con la llegada de internet a nuestras vidas.

El origen de esta figura delictiva se viene situando en EE.UU., en la California del año 1990, y posteriormente en 1996 se extendería al resto de Estados como delito federal. Pero no sólo de ella se hace eco el mundo anglosajón, en países como Canadá o Reino Unido, sino que se sumaron otros de herencia jurídica continental como Alemania o Italia, y actualmente también España²⁷. Volviendo a California, la Sección 646-9 de su Código Penal, habla de acoso como un delito en el que un tercero asedia reiteradamente a otra persona con una finalidad dañosa, de tal manera que la víctima llega a temer por su seguridad, y esta conducta no sólo puede ser física sino también incluye la realizada a través de internet²⁸. A su propósito hay encuestas que denotan como el acoso es más frecuente de lo que comúnmente se pudiera pensar²⁹.

Este delito se introduce en el Código Penal por la LO 1/2015, de 30 de marzo, como delito de acoso. Se trata de comportamientos delictivos que, dada su trascen-

²⁶ Gobierno de España, Ministerio para la Transformación Digital y de la Función Pública, Secretaría de Estado de Digitalización e Inteligencia Artificial, «Indicadores de uso de inteligencia artificial en España 2024», *red.es, ontsi* (2025): 12-14.

²⁷ Jose M.ª Torras Coll, «El delito de stalking. Breves consideraciones», *Lefebvre-El Derecho.com* (mayo de 2017): sin paginación.

²⁸ Robert A. Guy, Jr., «The Nature and Constitutionality of Stalking Laws», 46 *Vanderbilt Law Review* 991 (1993): 3-41.

²⁹ Patricia Tjaden, y Nancy Thoennes, «Stalking in America: findings from the national violence against women survey», *U.S. Department of Justice-Office of Justice Programs*, NCJ n.º 169592 (1998): 1-19.

dencia, no podían subsumirse como simples amenazas o coacciones³⁰. Pero es que, a mayores, hay posteriores modificaciones del artículo que recogen este tipo penal, y se trata de la LO 10/2022, de 6 de septiembre, y de la LO 4/2023, de 27 de abril.

La vigilancia de la persona acosadora sobre la persona acosada puede hacerse de modo presencial, es decir con seguimientos por la calle, a la salida de casa, del puesto de trabajo, también con llamadas telefónicas obsesivas, pero desde el auge de las redes sociales está el *stalking* digital, con el cual ya no es preciso vivir en la misma ciudad para una la observación intimidatoria, invadiendo la esfera privada de alguien, y además este hecho por la propia esencia del delito no es algo puntual, y normalmente ni siquiera se desarrolla en períodos temporales cortos, sino que contrariamente viene siendo una actividad prolongada.

A mayor abundamiento, tratando de dilucidar cuales pueden ser las motivaciones que mueven a alguien a convertirse en un acosador digital, no parece descabellado pensar en conductas que ya desde su inicio son insanas o que se pueden tornar en tóxicas pasado un tiempo, es decir, puede tratarse de alguien que busca recuperar el afecto perdido o que trata de conquistar a alguien, pero que en cualquier caso lo hace de forma compulsiva, lo que denotaría algún trastorno afectivo; y también estaría esa persona cuyo rol es si cabe más peligroso, pues busca contactos de índole sexual.

En este orden de cosas, las redes sociales son las plataformas perfectas para consumir estas acciones, pues cuentan con múltiples factores que allanan el camino: por un lado, se posibilitan con gran facilidad contactos con personas que ni siquiera se conocen, y se hace por medio de servicios en redes sociales / además son muchas las ocasiones en las que de forma pueril, los usuarios de estos medios en línea cuelgan información privada como lugar de residencia, fotografías muy personales / lo cibernético por definición implica poca o nula claridad, por lo que las posibilidades de esconderse tras las redes y de ocultar sus intenciones son infinitas / cuando se produce un ilícito penal, la labor de investigación puede ser una carrera de fondo para los Cuerpos y Fuerzas de Seguridad del Estado, pues se viene convirtiendo en algo complejo y tardío de poder resolverse.

Los resultados de estas acciones para las víctimas son nefastos ya que trastocan la normalidad de su vida, dado que la persistencia es la tónica general de este tipo de delitos, pues que como se ha apuntado el victimario hace uso de diversas formas de acoso. Significativamente el delito de *stalking* se encuentra ubicado en el título VI delitos contra la libertad, dentro del capítulo III delitos de coacciones, y contemplado en el artículo 172-ter CP, y los actos constitutivos de esta figura delictiva, a los que se ha hecho referencia y vistos más detenidamente, se encuentran en el apartado uno y son los siguientes:

—Un primer supuesto es la vigilancia y persecución contumaz a un tercero sin autorización que le legitime, con búsqueda de cercanía física.

³⁰ Patricia Tapia Ballesteros, «Stalking: el delito de acoso, de acecho o predatorio (art. 172 ter CP). Problemas de delimitación del tipo penal en España», *Revista Penal* n.º 43 (diciembre de 2018): 172-195.

- Un segundo supuesto trata sobre el envío de mensajes a un tercero, a quien se conoce o no, y llevarlo a cabo por medio de *whatsapp* o redes sociales y demás medios de comunicación. Esta actividad tiene que realizarse insistentemente y sin la aprobación del destinatario, generándole malestar y hostigamiento. También se puede intentar contactar con alguien a través de la convivencia de otros.
- Un tercer supuesto aborda cuando se usa información personal de otra persona de forma torticera para la adquisición de bienes o servicios.
- Un cuarto supuesto es cuando se atenta contra bienes o contra la libertad de alguien, o cuando se le quiere causar un mal, atentando contra bienes o contra la libertad de otro que guarda cercanía con la persona a la que se quiere dañar.

En estos cuatro supuestos, la pena de prisión puede ir desde los tres meses hasta los dos años además de multa. En el caso de que la víctima contra la que se atenta a su libertad o bienes sea especialmente vulnerable por razón de edad, enfermedad, discapacidad u otra circunstancia, la pena de prisión podrá ir de seis meses hasta dos años.

Cuando se ejerza violencia física o psíquica sobre quien sea o haya sido cónyuge o persona relacionada por similar situación afectiva, o sobre descendientes, ascendientes, hermanos propios o del cónyuge o conviviente, también cuando se trate de personas con discapacidad que convivan con el agresor o que estén bajo la potestad, tutela y demás del cónyuge o conviviente, o cuando se trate de personas integradas en el núcleo familiar, o cuando se trate de personas que por ser vulnerables estén bajo guarda en centros públicos o privados, pues bien en estos casos, la pena de prisión puede ir de uno hasta dos años o puede ser una pena de trabajos en beneficio de la comunidad; y a esto se agrega que no habría necesidad de denuncia por parte de la víctima como sí sucede en el resto de los casos de *stalking*, pues la policía puede hacerlo cuando tenga constancia de ello.

Al hilo de lo anterior, el delito de *stalking* estaría configurado en la categoría de delito semipúblico o semiprivado, ya que por regla general requiere previa denuncia de la persona afectada para que pueda ser perseguido judicialmente; a excepción de lo expuesto en el anterior párrafo que pasaría a tener la consideración de delito público al poder ser perseguido de oficio.

- Un quinto supuesto de *stalking*, es cuando el autor del hecho delictivo, y sin permiso del titular, haga uso de la imagen de la víctima para abrir perfiles falsos en páginas de contacto, que origine al perjudicado una situación de acoso o humillación, pudiendo ser penado el delincuente con prisión desde tres meses hasta un año o con multa; y si el ofendido es un menor o un discapacitado se agravaría dicha condena.

Hay que añadir que en todos los supuestos en que el agraviado por el delito sea el que deba interponer la denuncia, sin embargo, cuando se precise, como es el

caso de una víctima con discapacidad o en caso de menores, será su representante legal el encargado de hacerlo.

Continuando con las penas, todas las mencionadas anteriormente se pueden imponer sin perjuicio de las que también correspondan a los delitos en los que los actos de acoso se hubieran concretado. En este sentido habría que diferenciar si se está ante un concurso ideal de delitos en que con un único acto se realizan varios delitos o ante un concurso real de delitos en que con varios actos enlazados dan lugar a la comisión de varios delitos distintos que parece ser su consideración más apropiada.

Cuando se produce un delito de *stalking* entre ex parejas, hayan sido o no cónyuges, siendo el autor un hombre y la víctima una mujer, podríamos estar ante un delito de violencia de género conforme se estipula en la LO 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género. De hecho, en su artículo 1-1 y 1-3, comprende la violencia contra las mujeres «por quienes sean o hayan sido sus cónyuges o de quienes estén o hayan estado ligados a ellas por relaciones similares de afectividad, aun sin convivencia» e incluye también «todo acto de violencia física y psicológica».

El ciberacoso guarda similitud con el *ciberbulling*, ya que se puede hacer uso de insultos que denigran al que los recibe, lo que da como resultado que su integridad se vea gravemente afectada, y se desestabilice tanto física como emocionalmente.

A este respecto, cabe citar alguna de las sentencias que el Alto Tribunal ha dictado sobre esta cuestión, y así nos encontramos con los siguientes fallos judiciales:

- STS 770/2006, que hace referencia a la agravación de este delito cuando haya existido una relación matrimonial o haya existido una relación *more uxorio*, pero que en el momento de los ataques ya hubiera desaparecido esa relación afectiva.
- STS 324/2017, que versa sobre el *stalking* y su tratamiento en el artículo 172 ter-2 CP, en la que se prevé que para que exista la consideración de este tipo de delito, debe darse reiteración en la conducta hostigadora además de que la misma se prolongue en el tiempo, y que dicho comportamiento sea de tal calado que obligue a la víctima a modificar su habitual modo de vida.
- STS 554/2017, de 12 de julio, en la cual se rechaza el recurso de casación interpuesto contra una sentencia de la Audiencia provincial de Madrid, y se confirma la sentencia condenatoria por un delito de acoso del artículo 172 ter, al referir la presencia de actos reiterativos contemplados en este tipo penal, toda vez que la persona agraviada vio alterada su vida normal, como consecuencia de estas actuaciones de acecho y tentativas de querencia para comunicarse con la víctima. El bien jurídico protegido en este delito es la libertad individual de actuación del ofendido, que ve menoscabada su seguridad al no poder vivir con la tranquilidad necesaria.

8. Perspectiva criminológica y su incardinación en distintas teorías

Para comprender qué perfiles engloban la personalidad de los ciberdelincuentes, habría que retroceder y profundizar sobre la etiología de este tipo de delitos, donde el oscurantismo y la celeridad son el santo y seña de su misma esencia. En la ciberdelincuencia, hay lobos solitarios que actúan por su cuenta y riesgo, pero en numerosas ocasiones suele existir una estructura organizativa que actúa siempre en línea o que actúa de forma híbrida. Y en estas actuaciones aparecen figuras como los codificadores, que crean programas maliciosos que detectan las debilidades de seguridad para atacar los sistemas informáticos. O asimismo están los piratas informáticos que se aprovechan de las vulnerabilidades en redes. Y un caso más específico como es el de abusos sexuales a menores, suelen utilizar a sus miembros para captar a estos niños³¹.

Una forma de esconderse es encriptar las actividades delictivas, que es el medio por el que se codifica determinada información para que sea ilegible y para que únicamente puedan leerlo las personas que con los mecanismos adecuados lo transformen a su formato inicial. También está el borrado en remoto, es decir, enviar un comando a un dispositivo móvil para la eliminación de algunos datos, hecho que se suele producir cuando un teléfono móvil u ordenador portátil ha sido robado³², o es digno de mención que se comercialicen teléfonos móviles alterados para dar seguridad en la comisión de delitos.

En la doctrina nos encontramos con autores que abordan estas cuestiones, y que pueden arrojar luz permitiendo al lector sacar sus propias conclusiones con las premisas que en cada tesis se plantee.

Las teorías criminológicas que a continuación se exponen, se adaptan al entorno digital para poder explicar los delitos que se cometen en un contexto virtual, *v.gr.* con la primera de las teorías que se exponen a continuación se explica lo que también sirve para las demás en función de lo que éstas manifiesten:

—Véase el caso de la teoría de las actividades cotidianas, que sostienen los criminólogos Lawrence Cohen y Marcus Felson en el tercer cuarto del siglo xx, en la que hay tres factores que influyen en la victimización, que son el ofensor dispuesto a ello, las víctimas proclives a serlo, y que no haya gentes que controlen el cumplimiento de las reglas, lo cual conduce a su conculcación, de forma que, aunque las condiciones socio-laborales y de vida sean mejores, esto no lleva consigo una disminución en los delitos, sino que contrariamente la interacción directa entre víctima y delincuente aumenta

³¹ Unodc Oficina de las Naciones Unidas contra la Droga y el Delito. *Compendio de ciberdelincuencia organizada* (Viena: Producción editorial: Sección de Servicios en Inglés, Publicaciones y Biblioteca, Oficina de las Naciones Unidas, 2022): 16–21.

³² NSYS Group Team, «¿Es el borrado remoto una excelente manera de borrar datos?», NSYS GROUP (febrero 2024): sin paginación.

y consecuentemente las oportunidades de delinquir³³. En este contexto, al igual que en la comisión de delitos no virtuales, se dan estos tres elementos. Del mismo modo sucede en la red, pues aun cuando se legisle sobre la materia y se trate de controlar los actos delictivos, es tan inmenso el espacio cibernético que resulta sencillo incurrir en un sinnúmero de tropelías. Pues bien, si la contextualización del crimen no fuera física, sino que se diera en el ámbito de lo digital, es fácilmente reconducible, ya que la víctima podría ser una red poco o nada protegida, el controlador inexistente podría ser porque no hubiera un equipo técnico idóneo (dentro de lo que llamamos TICs), y obviamente el sujeto que comete el crimen es el ciberdelincuente.

- Está lo que preconizó en su día el sociólogo norteamericano Edwin Sutherland con su Teoría de la Asociación Diferencial en la primera mitad del siglo xx, que aboga por un modelo de comportamiento criminal aprendido a través de la comunicación social, pues en este contexto se fragua un sistema de enseñanza-aprendizaje de comportamientos delictivos tanto de las técnicas como de las actitudes³⁴. En consecuencia, qué duda cabe sino pensar que la web es un espacio virtual propicio para que ello ocurra.
- Otros postulados defienden la Teoría de la Neutralización, de modo que los criminólogos David Matza y Gresham Sykes hacia mil novecientos cincuenta, convinieron en afirmar que la delincuencia juvenil está a caballo entre el respeto a las normas y su vulneración a sabiendas de que esto último está mal, por tanto no hay desconocimiento en dicha transgresión, aunque sin embargo hay líneas rojas que pueden ser no dañar a su entorno más cercano como familia o amigos, ni atentar contra determinados valores como son los de carácter religioso³⁵.
- Para los sociólogos y criminólogos estadounidenses Gottfredson y Hirschi, es el control de los impulsos lo determinante en la eliminación de la delincuencia. Fue a finales del siglo xx cuando Michael Gottfredson y Travis Hirschi, analizan que a los que delinquen les mueve el cortoplacismo, y delinquir les genera una recompensa, en tanto en cuanto se puedan obtener beneficios dinerarios, sexuales, ajustes de cuentas, el mal por el mal, etcétera; sin embargo, hay otra parte de la población que cultiva el autocontrol tanto en beneficio propio como porque son respetuosos con el dolor ajeno³⁶.

³³ Lawrence E. Cohen y Marcus Felson, «Social Change and Crime Rate Trends: A Routine Activity Approach», *American Sociological Review*, 44, n.º 4 (1979): 588-608.

³⁴ Wael Hikal, «La Teoría de la Asociación Diferencial para la Explicación de la Criminalidad y la Articulación de una Política Criminal», *Derecho y Cambio Social* (2017): 1-15.

³⁵ Gresham M. Sykes y David Matza, «Techniques of Neutralization: A Theory of Delinquency», *American Sociological Review*, 22, n.º 6 (1957): 664-670.

³⁶ Miguel A. Villavieja Beck y Ana I. Cerezo Domínguez, «La Piratería Doméstica y el Autocontrol: Un Estudio Exploratorio entre Universitarios», *Boletín Criminológico-Instituto Andaluz Interuniversitario de Criminología*, n.º 22 (2016): 3-9. Travis Hirschi y Michael Gottfredson, «Commentary: testing the general theory of crime», *Sage Journals*, 30, n.º 1 (1993): 47-54. Ronald L. Akers, «Self-Control as a General Theory of Crime», *Journal of Quantitative Criminology* 7, n.º 2 (1991): 201-211. Alfonso SerranoMaíllo y Christopher H. Birbeck, *La Generalidad de la Teoría del Autocontrol* (Madrid: Dykinson, 2014).

- Otras opiniones en torno a este tema, son las que abanderan el castigo como medida disuasoria en la comisión de crímenes, tal es así que el jurista italiano del siglo XVIII Cesare Beccaria, baluarte del moderno Derecho Penal en Europa, recogía la idea de cuándo el potencial delincuente se inhibe de llevar a cabo una acción delictiva, y es que si al evaluar el coste-beneficio concluye que la sanción será mayor a la gratificación que pueda conseguir, esto hará que se deseché la idea de cometer actos delictivos, siendo por tanto la pena un elemento de prevención³⁷. En el terreno de la ciberdelincuencia, pese a ser delitos que ya se encuentran en la sociedad desde hace años, todavía puede considerarse un modelo de criminalidad nuevo, pero la normativa reguladora y sancionadora intensifica sus esfuerzos para tratar de dar cobertura legal a estos hechos.
- James Q. Wilson y George L. Kelling elucubran con la Teoría de las Ventanas Rotas en el último cuarto del siglo XX³⁸, y es el psicólogo norteamericano Philip Zimbardo quién realiza un experimento. Esta hipótesis contempla la idea de que cuando la delincuencia se visibiliza trae como resultado mayores conductas delictivas y caos social en la comunidad³⁹. Esta afirmación parece de sentido común, pues el seguidismo funciona en todos los ámbitos, y por inverosímil que pueda parecer también lo hace en lo que al crimen se refiere.
- Otro posicionamiento teórico, es el que formuló el sociólogo estadounidense Robert Agnew hacia 1990, y que denominó Teoría de la Tensión, la cual tiene antecedentes en otros estudiosos de la Sociología, como lo fue Robert K. Merton a principios del siglo XX. El contenido de la misma es la relación entre delincuencia y entorno, siendo las relaciones que provocan efectos negativos y frustrantes las que hacen que las personas puedan desembocar en actuaciones delictivas⁴⁰. Sin duda las reacciones no tienen por qué ser coincidentes en escenarios similares, pero hay momentos en que sí se repiten, y la manera de encajar las vicisitudes y avatares adversos que la vida pone en el camino, dependiendo de otras variables, como el carácter, la situación personal, familiar, socio-laboral, hacen que se puedan producir conductas que entran de lleno en tipos penales. A esto se suma, todo lo que internet ofrece, positivo o negativo, y siendo esto último lo que nos ocupa, casi cualquier persona en nuestros días tiene acceso a un ordenador, y dependiendo de su pericia en el manejo, podrán cometerse delitos más o menos sofisticados.

³⁷ Edison Carrasco-Jiménez, «Cesare Beccaria y la Percepción (Estética) como Fundamento en su Política-Criminal», *International Institute of Humanities, Cultural Criticism and Social Sciences-Ideas y Valores*, LXXI, n.º 181 (2023): 63-80. Cesare Beccaria, *De los Delitos y de las Penas* (Madrid: Tecnos, 2008).

³⁸ George L. Kelling y James Q. Wilson, «Broken Windows. The police and neighborhood safety», *The Atlantic* (marzo de 1982): sin paginación.

³⁹ Óscar Castellero Mimenza. «La teoría de las ventanas rotas y el experimento de Zimbardo», *Psicología y Mente* (marzo de 2018): sin paginación.

⁴⁰ Marco Teijón Alcalá, «La General Strain Theory y las Políticas Criminales», en *Propuestas Penales: Nuevos Retos y Modernas Tecnologías* (Salamanca: Universidad de Salamanca, 2016), 755-772.

Cabe abordar el perfil criminal de un ciberdelincuente, y pese a haber motivaciones distintas dependiendo de cosas como el tipo de delito, sí parecen existir particularidades coincidentes en el carácter como introversión, narcisismo, psicoticidad que provoca soledad, falta de empatía, inhabilidades sociales, ansias de control, agresividad. Otros rasgos de los ciberdelinquentes son su elevado nivel educativo y la buena opinión que tienen de sí mismos ⁴¹. El espacio virtual es un nicho para el ciberdelincuente, pues presenta gran facilidad para el encubrimiento, las lagunas en la legislación y la poca o nula cercanía de las víctimas representa una sensación de impunidad, ya que el hecho delictivo se puede perpetrar desde cualquier punto del globo terrestre. Véanse las más destacadas clases de criminalidad ciberespacial entre 2015 y 2019⁴²:

Años	Año 2019	Año 2018	Año 2017	Año 2016	Año 2015
Delitos de acceso e interceptación ilícita	4.004	3.384	3.150	3.243	2.893
Delitos de amenazas y coacciones	12.782	12.800	11.812	12.036	10.607
Delitos contra el honor	1.422	1.448	1.561	1.546	2.205
Delitos contra la propiedad intelectual	197	232	121	129	172
Delitos sexuales	1.774	1.581	1.392	1.231	1.306
Delitos de falsificación informática	4.275	3.436	3.280	3.017	2.644
Delitos de fraude informático	192.375	136.656	94.792	70.178	62.038
Delitos de interferencia en datos y sistemas	1.473	1.192	1.291	1.336	1.193
TOTAL	218.302	160.729	117.399	92.716	83.058

Fuente: tabla de elaboración propia, extraída la información de *Cuadernos de RES PÚBLICA en Derecho y Criminología*.

9. Perspectiva victimológica

Teniendo en cuenta que parece que vivimos en una sociedad del riesgo⁴³, de tendencia globalizante y que no se circunscribe a fronteras, en ella aparecen igualmente amenazas globales.

La víctima es parte esencial de cualquier delito, y no podía ser menos en el ciberdelito⁴⁴. Desde el punto de vista de la victimología cibernética, el universo di-

⁴¹ Vicente Garrido Genovés y Santiago Redondo Illescas, *Principios de Criminología* (Valencia: Editorial Tirant lo Blanch, 2023), 37 y 38.

⁴² Víctor Rodríguez González, Claudio Augusto Payá Santos y Bernardo Peña Herrera, «Estudio criminológico del ciberdelincuente y sus víctimas», *Cuadernos de RES PÚBLICA en Derecho y Criminología*, n.º 1 (mayo de 2023): 1-13.

⁴³ Ulrich Beck, *La sociedad del riesgo* (Barcelona: Paidós, 2006).

⁴⁴ Luis Miguel Reyna Alfaro, «Criminalidad informática, crimen organizado e internacionalización del delito», en *Ley contra el crimen organizado (Ley n.º 30077)* (Lima: Instituto Pacífico S.A.C., 2016), 197-236.

gital por su complejidad tiene características que cualquier profano en la materia puede visibilizar, como son:

- La no existencia de barreras físicas hace que se produzca una globalización del delito, es decir que se amplíen exponencialmente los lugares a los que el crimen puede llegar.
- Se añade, que aún hoy en día hay un salto cualitativo y cuantitativo generacional que conlleva ignorancia en el conocimiento de las herramientas virtuales, lo que aumenta el número de personas proclives a adquirir el rol de víctima.
- El anonimato implica el desconocimiento de la persona con la que se interactúa al otro lado de la pantalla.
- Como se ha expuesto, el número de delitos ha aumentado ya no sólo en cantidad sino en la presencia de nuevas tipologías.
- Es de sentido común y de justicia reconocer el impacto que un delito puede provocar en la vida y en la salud, física y mental del agraviado, pero es que las redes además tienen la capacidad de ser una ventana al mundo y por consiguiente de dar visibilidad a algunas de estas conductas lesivas, y esto es un terreno fértil para que los efectos psicológicos dañosos se multipliquen, y es lo que haciendo una traslación con el proceso penal y en este caso con el victimario llamaríamos «la pena de banquillo».
- Otro elemento añadido, es que al igual que ocurre con los delitos digamos presenciales, también y quizás aún más si se tiene en cuenta el número de delitos virtuales, es que no son pocos los que por vergüenza no se denuncian.

10. Conclusiones

Como se ha puesto de manifiesto en la exposición de las teorías criminológicas, los planteamientos que sus precursores hicieron en el pasado son plenamente aplicables a la actualidad y a los tipos penales cibernéticos, y de cada una de ellas se pueden extraer conclusiones que ayuden a comprender las motivaciones de los delincuentes, las lagunas legales y los puntos vulnerables que hacen que las víctimas lo sean.

A la vista de la información analizada, resta concluir que nos encontramos en la era de la tecnología, y que la delincuencia ha dado en los últimos años un giro copernicano. Lo tecnológico bien empleado aporta bondades, pero hay una cara oculta tóxica a la que perseguir y si se puede, adelantarse a sus maniobras delictivas a través de la ciberseguridad, con el uso de herramientas como la *big data* que permite analizar datos masivos generados en internet por los usuarios de las redes, y supone para las organizaciones prever ataques a través de la determinación de patrones de conducta.

En la comisión de cualquier delito, existen conductas que se repiten, pero la diferencia que ayuda a la ciberdelincuencia es precisamente la posibilidad de ocultación que anonimiza al autor, por lo que se trata de averiguar cuál es la huella digital

que lleve a los investigadores a descubrir su verdadera identidad, empleando algoritmos que detecten y neutralicen amenazas. Por éste y otros motivos, los países adoptan medidas legales al servicio de su tratamiento, basados en la cooperación internacional, pero además internamente cada Estado, adapta las leyes penales y procedimentales para esta nueva realidad delictiva.

En el epítome de lo expuesto, cabe decir que si se hace un recorrido de control de seguridad de mayor a menor, estarían los anteriormente nombrados mecanismos legales internacionales o nacionales, y en el siguiente escalafón estaría el especial cuidado que cada cual mantenga en su vida diaria en el uso de las nuevas tecnologías, y con especial celo está la vigilancia de las actividades que niños y jóvenes lleven a cabo a través de las redes.

Hay que añadir que acotar jurídicamente los delitos cometidos en el entorno digital, es verdaderamente complicado, pues el Ordenamiento Jurídico resulta lento en relación a la evolución social. Este ámbito presenta problemáticas claramente definidas, pues ni existe un único bien jurídico a proteger, ni existe un único perfil criminológico, y ni siquiera es posible calibrar las incidencias victimológicas.

11. Fuentes

11.1. Normas

Circular 3/2017, de 21 de septiembre, de la Fiscalía General del Estado sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos.

Constitución Española, de 29 de diciembre de 1978.

Convenio de Budapest sobre ciberdelincuencia, de 23 de noviembre del 2001.

Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio del 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre del 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

Instrucción 10/2005, de la Fiscalía General del Estado, sobre el tratamiento del acoso escolar desde el sistema judicial juvenil.

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

- Ley 13/2015, de 5 de octubre, de reforma de la Ley de Enjuiciamiento Criminal, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.
- LO 10/1995, de 23 de noviembre, del Código Penal.
- LO 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género.
- LO 1/2015, de 30 de marzo, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal.
- LO 10/2022, de 6 de septiembre de Garantía Integral de la Libertad Sexual.
- LO 4/2023, de 27 de abril, que modifica la LO 10/1995 del Código Penal en relación con los delitos contra la libertad sexual.
- Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (Texto pertinente a efectos del EEE).
- Tratado Internacional sobre delitos cibernéticos de 25 de diciembre de 2024, adoptado por la Asamblea General de las Naciones Unidas.

11.2. Sentencias

- STS 819/2002, de 8 de mayo (Sala de lo Penal), siendo ponente el Excmo. Sr. D. Julián Sánchez Melgar, ECLI:ES:TS:2002:3247.
- STS 1218/2004, de 2 de noviembre (Sala de lo Penal), siendo ponente el Excmo. Sr. D. Juan Ramón Berdugo Gómez de la Torre, ECLI: ES:TS:2004.7040.
- STS 770/2006, de 13 de julio (Sala de lo Penal, Sección 1.ª), siendo ponente el Excmo. Sr. D. Juan Ramón Berdugo Gómez de la Torre, ECLI:ES:TS:2006:6182 y N.º de Recurso 1471/2005.
- SAP Málaga 452/2009, de 16 de septiembre, siendo ponente el Excmo. Sr. D. Julio Manuel Ruiz-Rico Ruiz-Morón, ECLI: ES: APMA:2009:1883.
- STS 324/2017, de 08 de mayo (Sala de lo Penal), siendo ponente el Excmo. Sr. D. Antonio del Moral García, Roj:STS 1647/2017, ECLI:ES:TS:2017:1647 y N.º de Recurso 1775/2016.
- STS 554/2017, de 12 de julio (Sala de lo Penal, Sección 1.ª), siendo ponente el Excmo. Sr. D. Joaquín Giménez García, Roj:STS 2819/2017, ECLI:ES:TS:2017:2819 y N.º de Recurso 1745/2016.

STS 377/2018, de 23 de julio (Sala de lo Penal), siendo ponente el Excmo. Sr. D. Vicente Magro Servet, Roj:TS 3040/2018, ECLI:ES:TS:2018:3040 y n.º de Recurso 10036/2018 P.

SAN 8/2020, de 15 de septiembre (Sala de lo Penal), siendo ponente la Excm. Sra. Dña Manuela Francisca Fernández Prado, ECLI:ES:AN:2020:4293 y n.º de Recurso 8/2020.

12. Bibliografía y otras fuentes

AKERS, Ronald L. «Self-Control as a General Theory of Crime», *Journal of Quantitative Criminology* 7, n.º 2 (1991): 201-211.

ÁLVAREZ CALDERÓN, Carlos Enrique. *La arquitectura ilícita del ciberespacio: cibercrimen y ecosistemas de la dark web. En C.E. El campo de batalla digital: la defensa nacional en la era algorítmica, Vol. I Infraestructuras de la guerra digital: computación, ciber guerra y defensa del ciberespacio*. Bogotá: ESDEG, 2026.

ARÉVALO, María Camila. «ISO 27032, el estándar enfocado en ciberseguridad», *Pirani* (2020): sin paginación.

ATHIE CERVANTES, Adolfo *et al.* «Aprobación del Primer Tratado Intenacional en Materia de Cibercrimen», *NOTI BASHAM* (enero de 2025): sin paginación.

BAJO-PÉREZ, Irene. «Ciberviolencias machistas en Instagram: relación entre el número de seguidores y seguidoras y la violencia recibida». En *Feminismo Digital. Violencia contra las mujeres y brecha sexista en Internet*, 711-730. Madrid: Dykinson, 2021.

BECCARIA, Cesare. *De los delitos y de las penas*. Madrid: Tecnos, 2008.

BECK, Ulrich. *La sociedad del riesgo*. Barcelona: Paidós, 2006.

CARRASCO-JIMÉNEZ, Edison. «Cesare Beccaria y la Percepción (Estética) como Fundamento en su Política-Criminal», *International Institute of Humanities, Cultural Criticism and Social Sciences-Ideas y Valores LXXI*, n.º 181 (2023): 63-80.

CASTILLERO MIMENZA, Óscar. «La teoría de las ventanas rotas y el experimento de Zimbardo», *Psicología y Mente* (marzo de 2018): sin paginación.

CASTRO, Abraham y CARBALLO, Eva. «Cuestiones más significativas de la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual», *Legal Today* (octubre de 2022): sin paginación.

CERVERA, Alfonso. «Todo lo que necesitas saber sobre Worm GPT», *Recoverit* (mayo de 2026): sin paginación.

CIDONCHA ROMERO, Dolores Cidoncha y DE LA CRUZ FORTUN, M.ª Ángeles. *La violencia sexual y las nuevas tecnologías. Guía para jóvenes y adolescentes*. Zaragoza: Instituto Aragonés de la Mujer Gobierno de Aragón, 2023.

COHEN, Lawrence E. y Felson, MARCUS. «Social Change and Crime Rate Trends: A Routine Activity Approach», *American Sociological Review* 44, n.º 4 (1979): 588-608.

- DRAPER, John T. et al. *Beyond The Little Blue Box: The Biographical Adventure of John T. Draper (Aka Captain Crunch). Notorious «phone Phreak», Legendary Internet Pioneer and Ardent Privacy Advocate*. Canadá: Friesen Press, 2018. 30-200.
- GARRIDO GENOVÉS, Vicente y REDONDO ILLESCAS, Santiago. *Principios de Criminología*, Valencia: Tirant lo Blanch. 2023.
- GOBIERNO DE CANARIAS, <https://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/producto/el-caso-de-amanda-todd-subtitulado/>
- GOBIERNO DE ESPAÑA, Ministerio para la Transformación Digital y de la Función Pública, Secretaría de Estado de Digitalización e Inteligencia Artificial, «Indicadores de uso de inteligencia artificial en España 2024» *red.es, ontsi* (2025): 12-14.
- GUY J. R., Robert A. «The Nature and Constitutionality of Stalking Laws», 46 *Vanderbilt Law Review* 991 (1993): 3-41.
- HERRERA MORENO, Miriam y SÁNCHEZ RUBIO, Beatriz. *Criminalidad, desviación y riesgo en la ludosfera: Nuevas dinámicas de recreación digital dañina*, Madrid: Dykinson, 2025.
- HIKAL, Wael. «La Teoría de la Asociación Diferencial para la Explicación de la Criminalidad y la Articulación de una Política Criminal», *Derecho y Cambio Social* (2017): 1-15.
- HIRSCHI, Travis y GOTTFREDSON, Michael. «Commentary: testing the general theory of crime», *Sage Journals* 30, n.º 1 (1993): 47-54.
- JIMÉNEZ HERNÁNDEZ, Antonio Salvador et al. *Participación, políticas sociales y protección de la infancia. Aprendiendo con los niños y las niñas a construir sociedades inclusivas*, España: CIPI, 2018.
- JULIÁN, Guillermo. «Stuxnet: historia del primer arma de la ciberguerra», *Genbeta* (diciembre de 2013): sin paginación.
- KELLING, George L. y WILLSON, James Q. «Broken Windows. The police and neighborhood safety», *The Atlantic* (marzo de 1982): sin paginación.
- LANIER, Kevin. «Storm-0558 Forensic Analysis», *Cyber* (marzo de 2025): sin paginación.
- LÓPEZ JIMÉNEZ, Raquel. *Victimización sexual y nuevas tecnologías: desafíos probatorios*. Madrid: Dykinson, 2021.
- MARTÍNEZ ROMÁN, Rosana, RODRÍGUEZ CASTRO, Yolanda y LAMEIRAS FERNÁNDEZ, María. «Grooming, sexting y sextorsión, los nuevos fenómenos de ciberviolencia: la coeducación como media de prevención». En *Ensayos Ciberfeministas*, 52-67. Madrid: Dykinson, 2023.
- MONTIEL, Juan, Irene y CARBONELL VAYA, Enrique J. y SALOM GARCÍA, Miriam. «Victimización Infantil Sexual Online: Online Grooming, ciberabuso y ciberacoso sexual». En *Delitos sexuales contra menores. Abordaje psicológico, jurídico y policial*, 223-224. Madrid: Tirant lo Blanch, 2014.
- MONTILLA AGUILERA, Francisco Javier. «El ciberespacio desde la perspectiva china: análisis estratégico y operacional», *RDEN Revista de Estudios Internacionales* (mayo de 2025): sin paginación.

- NAVA GARCÉS, Alberto Enrique. «El caso Wannacry. Ataque en la red», *Revista Penal*, n.º 42 (julio 2018), 148-164.
- NSYS GROUP TEAM, «¿Es el borrado remoto una excelente manera de borrar datos?», NSYS GROUP (febrero de 2024): sin paginación.
- NEWMeyer, Kevin P. «Cyber Espionage: A threat to National Security», *Center for Hemispheric Defense Studies Security and Defense Studies Review An Interdisciplinary Journal*, 10 (2010): 113-122.
- NEYRA CASTILLA, Orietta Mireya (2021), «Ciberbullying: El acoso escolar en el ciberespacio e implicancias psicológicas», *Hamut'ay* 8, n.º1 (2021): 67-74.
- REJAS DE LA PEÑA, Aldo Fernando *et al.* «La Inteligencia Artificial en la lucha contra el crimen organizado», *Ciencia Latina*, n.º 4 (2024): 2144-2158.
- REYNA ALFARO, Luis Miguel. «Criminalidad informática, crimen organizado e internacionalización del delito». En *Ley contra el crimen organizado (Ley N.º 30077)*, 197-236. Lima: Instituto Pacífico S.A.C., 2016.
- RODRÍGUEZ DOMÍNGUEZ, Carmen y DURÁN SEGURA, Mercedes. «Sextorsión: nueva forma de violencia hacia chicas adolescentes». En *Participación, políticas sociales y protección de la infancia: aprendiendo con los niños y las niñas a construir sociedades inclusivas*, 128-136. Sevilla: CIPI, 2018.
- RODRÍGUEZ GONZÁLEZ, Víctor, PAYA SANTOS, Claudio Augusto y PEÑA HERRERA, Bernardo. «Estudio criminológico del ciberdelincuente y sus víctimas», *Cuadernos de RES PÚBLICA en Derecho y Criminología*, n.º 1 (mayo de 2023): 1-13.
- ROMEO CASABONA, Carlos M.^a. *De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal* (Salamanca: Universidad de Salamanca, 2006), 1-43.
- RUILOBA-NÚÑEZ, Juana M.^a. «Acciones públicas frente a la violencia de género digital. Un acercamiento comparado desde el nivel autonómico español». En *Feminismo Digital. Violencia contra las mujeres y brecha sexista en internet*, 398-420. Madrid: Dykinson, 2021.
- RUANOVA ARANAZ, Ana M.^a. «Regulación de la Inteligencia Artificial: Europa abre el camino», *Abogacía de Valladolid – Revista semestral del Ilre. Colegio de la Abogacía de Valladolid* (2025): 38-39.
- SÁNCHEZ MEDERO, Gema. «El ciberespionaje», *Derecom-Nueva Época* (2013): 115-124.
- SERRANO MAILLO, Alfonso y BIRBECK, Christopher H. *La Generalidad de la Teoría del Autocontrol*. Madrid: Dykinson, 2014.
- SUÁREZ DE LA TORRE, Mercedes. «Ciberespionaje: una nueva forma de ataque y de defensa cibernética», *Antenas Neológicas-Red de neología del español* (marzo de 2016): sin paginación.
- SYKES, Gresham M. y MATZA, David. «Techniques of Neutralization: A Theory of Delinquency», *American Sociological Review* 22, n.º 6 (1957): 664-670.

- TAPIA BALLESTEROS, Patricia. «Stalking: el delito de acoso, de acecho o predatorio (art. 172 ter CP). Problemas de delimitación del tipo penal en España», *Revista Penal* n.º 43 (diciembre de 2018): 172-195.
- TEIJÓN ALCALÁ, Marco. «La General Strain Theory y las Políticas Criminales». En *Propuestas Penales: Nuevos Retos y Modernas Tecnologías*, 755-772. Salamanca: Universidad de Salamanca, 2016.
- TJADEN, Patricia y THOENNES, Nancy. «Stalking in America: findings from the national violence against women survey», *U.S. Department of Justice-Office of Justice Programs*, NCJ n.º 169592 (1998): 1-19.
- TORRAS COLL, José M.^a. «El delito de stalking. Breves consideraciones», *Lefebvre-El Derecho.com* (mayo de 2017): sin paginación.
- UNODC OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO. *Compendio de ciberdelincuencia organizada*, Viena: Producción editorial: Sección de Servicios en Inglés, Publicaciones y Biblioteca, Oficina de las Naciones Unidas, 2022.
- UNTIVEROS, Sergio. «ISO 27001 vs NIST: un análisis comparativo y su complementariedad», *Aprenda Redes* (noviembre de 2023): sin paginación.
- VALENZO SALGADO, María Guadalupe. «Inteligencia Artificial como instrumento del crimen organizado transnacional», *Ibero-Ciencias Revista Científica y Académica*, n.º especial UAGro (junio de 2026): 1-16.
- VILLAVIEJA BECK, Miguel A. y CEREZO DOMÍNGUEZ, Ana I. «La Piratería Doméstica y el Autocontrol: Un Estudio Exploratorio entre Universitarios», *Boletín Criminológico-Instituto Andaluz Interuniversitario de Criminología*, n.º 22 (2016): 3-9.