8. CRIMINALIDAD INFORMÁTICA

8.1 **Introducción**

La utilización de las redes y sistemas informáticos con fines ilícitos ha continuado incrementándose en el último periodo anual siguiendo la trayectoria ascendente de los últimos años. La ciberdelincuencia se va expandiendo progresivamente alcanzando a múltiples y variadas manifestaciones criminales y supone ya, según el Balance de Criminalidad del Ministerio del Interior correspondiente al cuarto trimestre del año 2025, el 19,85% de la actividad delictiva en nuestro país, con un índice de crecimiento del 5,3% respecto del año 2024. Es incuestionable, por tanto, que una buena parte de la actividad criminal se está desplazando inexorablemente al entorno digital.

Este imparable ascenso, del que venimos dando cuenta en anteriores memorias, se explica fácilmente a partir de la profunda digitalización de nuestra sociedad y del imparable desarrollo de la ciencia y la tecnología. Los datos no pueden ser más evidentes. Según el último informe publicado el pasado año por la Unión Internacional de Telecomunicaciones (UIT) de las Naciones Unidas, el número de personas que utilizan internet es de casi 6.000 millones –aproximadamente tres cuartas partes de la población mundial–. En nuestro país, el INE cifra en un 92,5% el porcentaje de ciudadanos y ciudadanas de entre 16 y 74 años que en 2025 usaron diariamente internet, en un 59,6% quienes realizaron *online* operaciones económicas de cualquier tipo y en un 37,9% los que utilizan, aun esporádicamente, la inteligencia artificial (en adelante, IA). Es claramente perceptible que, en los últimos años y, en particular tras la pandemia de la COVID-19, los seres humanos, aun con diferencias significativas en razón a ámbitos geográficos, hemos ido trasladando al entorno virtual muchas de las relaciones interpersonales, al igual que almacenamos y tratamos información de todo tipo en dispositivos y sistemas informáticos y desarrollamos *online* muchas de nuestras actividades habituales.

Por su parte, la rápida evolución de las tecnologías ha puesto a nuestra disposición potentes herramientas que hacen posible un nivel de conectividad inimaginable hasta hace unos pocos años al tiempo que facilitan la vida de las personas y contribuyen al florecimiento social, cultural y económico, al desarrollo de los pueblos y al progreso de la humanidad, pero que también pueden ser utilizadas irregularmente o con finalidades perversas, dando lugar a nuevos riesgos y amenazas para la seguridad de todos, para el normal funcionamiento de organismos, instituciones y empresas, e incluso para el

pleno ejercicio de los derechos y libertades que nos corresponden como personas.

La confluencia de ambos factores, junto con las tensiones geopolíticas y las innegables deficiencias en los sistemas de prevención y/o en las medidas de seguridad que hubieran debido adoptarse en el uso de estas herramientas, ha determinado un aumento en la superficie de ataque, así como nuevas y más peligrosas amenazas para la ciberseguridad, entre ellas las amenazas híbridas [13], y una mayor vulnerabilidad de la ciudadanía frente a las agresiones provenientes del ciberespacio. En los últimos años hemos ido constatando el imparable crecimiento de los ciberataques –*ransomware, DDoS, man-in-the-middle*–, con un perjuicio que se calcula en más de ocho billones de euros en 2025; la aparición de nuevas formas de defraudación vinculadas al uso irregular de instrumentos de pago distintos del efectivo y facilitadas por el auge del comercio electrónico; el robo de los datos de millones de personas y su puesta a disposición de terceros en mercados *online*; el uso del ciberespacio para diseminar *fake news* especialmente diseñadas para la desestabilización de organismos, instituciones e incluso de los Estados, y un preocupante incremento de las ciberagresiones a bienes personalísimos, particularmente de los más vulnerables como los niños, niñas y adolescentes y las mujeres como víctimas de la violencia de género.

En esta situación, la efectiva incidencia de las posibilidades ofensivas de la IA resulta todavía impredecible. Su potencial capacidad –a partir de mecanismos de aprendizaje automático– para identificar vulnerabilidades y brechas en los sistemas informáticos o alterar el comportamiento de sus algoritmos; articular campañas de *phishing* más convincentes; suplantar identidades ajenas con finalidades diversas; infringir derechos de propiedad intelectual; facilitar el acceso con objetivos criminales a los más vulnerables o elaborar y difundir material de abuso sexual infantil, es por el momento difícil de valorar, pero ya está mostrando sus primeros y peligrosos efectos lesivos.

La necesidad de afrontar eficazmente estos riesgos y amenazas para proteger los derechos y libertades de todos y los principios básicos de las sociedades democráticas está dando lugar a un intenso desarrollo legislativo nacional e internacional y a una constante adaptación de las estructuras y mecanismos de seguridad de toda clase de entidades, organismos e instituciones. Precisamente con ese objetivo, a principios de este año 2026, la Comisión Europea presentó un paquete de

[13] Son aquellas en las que se combinan las campañas de desinformación con los ataques a las infraestructuras críticas y/o a los organismos esenciales.

medidas para reforzar la resiliencia de redes y sistemas en el ámbito comunitario, en un contexto marcado por ataques cibernéticos e híbridos cada vez más frecuentes contra servicios esenciales, infraestructuras críticas e instituciones democráticas, no solo por parte de organizaciones criminales de carácter tradicional, sino también de atacantes respaldados y/o apoyados por autoridades estatales de determinados países.

El eje central de este proyecto es actualizar el Reglamento sobre la Ciberseguridad [14] con la finalidad de fortalecer la seguridad de las cadenas de suministro de las TIC, garantizar que los productos y servicios digitales disponibles al público incorporen por diseño mecanismos de ciberseguridad y mejorar la protección de las infraestructuras críticas. También se pretende con esta propuesta potenciar las capacidades de la Agencia de la UE para la Ciberseguridad (ENISA) a efectos de apoyar a los Estados miembros y a la propia Unión en la gestión de las amenazas provenientes del ciberespacio.

Este proyecto es un paso más en las medidas ya adoptadas en 2025, entre ellas la publicación del Reglamento de Cibersolidaridad [15], orientado a mejorar las capacidades de la Unión en la detección de amenazas e incidentes de seguridad, o la adopción por el Consejo en el mes de junio de un Plan Director de la UE para la Gestión de Crisis de Ciberseguridad.

Estas disposiciones complementan a su vez el acervo normativo ya vigente en esta materia en el territorio comunitario, en el que se incluyen, entre otras muchas disposiciones, la Directiva (UE) 2022/2555, de 14 de diciembre –Directiva NIS 2–, orientada a reforzar la resiliencia de redes y sistemas informáticos a partir de la estandarización de las medidas de seguridad exigibles a operadores y prestadores de servicios esenciales y el establecimiento de un sistema de notificación obligatoria de incidentes de seguridad o también el Reglamento de Servicios Digitales [16] y el Reglamento (UE) 2021/784, *sobre la lucha contra la difusión de contenidos terroristas en línea*,

---

[14] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, *relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013.*

[15] Reglamento (UE) 2025/38 del Parlamento Europeo y del Consejo, de 19 de diciembre de 2024, *por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar ciberamenazas e incidentes, prepararse y responder a ellos y por el que se modifica el Reglamento (UE) 2021/694.*

[16] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, *relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE.*

ambos con clara incidencia en la lucha contra la ciberdelincuencia ya que concretan y definen las obligaciones de los prestadores de servicios ante los requerimientos efectuados por autoridades competentes a efectos de la protección de aquellos bienes jurídicos que puedan verse afectados por actuaciones irregulares o ilícitas.

Al tiempo, la preocupación generada en los organismos comunitarios por los efectos perversos del uso irregular de la IA determinó la publicación del Reglamento de Inteligencia Artificial [17], por el que se establecen normas armonizadas para garantizar que su utilización no interfiera negativamente en la salud, la seguridad y el pleno respeto de los derechos de todas las personas, cualquiera que sea su clase, condición o características. Dichas normas, que ofrecen un enfoque basado en niveles de riesgo, están siendo implementadas en forma gradual en el territorio comunitario bajo la supervisión de la Oficina Europea de Inteligencia Artificial, creada específicamente con dicho objetivo.

En lo que aquí interesa, uno de los efectos derivados de esta profunda transformación social es la utilización de los avances tecnológicos para la planificación y ejecución de actividades criminales. Por ello, en los últimos años se están realizando grandes esfuerzos normativos en el ámbito comunitario para articular una respuesta uniforme y coordinada contra la ciberdelincuencia. Así, con apoyo en el art. 83 del Tratado de Funcionamiento de la Unión Europea, se han ido dictando diversas disposiciones orientadas a impulsar una política penal común frente a aquellas actividades delictivas que se consideran más peligrosas y que se han visto más favorecidas por la progresiva digitalización social. Es el caso, entre otras, de la Directiva (UE) 2011/93, de 13 de diciembre, *relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil;* la Directiva (UE) 2013/40, de 12 de agosto, *relativa a los ataques contra los sistemas de información*; la Directiva (UE) 2017/541, de 15 de marzo, *relativa a la lucha contra el terrorismo,* o la Directiva (UE) 2019/713, de 17 de abril, *sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo.*

La más reciente de ellas es la Directiva (UE) 2024/1385, de 14 de mayo, *sobre la lucha contra la violencia contra las mujeres y la violencia doméstica*, pendiente todavía de implementarse en nuestro país,

---

[17] 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.*

en la que se incluyen propuestas de especial valor a efectos de mejorar nuestra capacidad de actuación frente a la violencia de género digital. Así, en sus arts. 5 a 9 se definen como delitos conductas tales como la difusión no consentida de material íntimo o manipulado artificialmente; la vigilancia electrónica no autorizada (ciberacecho); el ciberacoso; el ciberexhibicionismo y la incitación a la violencia o al odio por medios cibernéticos, al tiempo que en su art. 23 se exhorta a los Estados a la adopción de medidas para eliminar contenidos ilícitos *online* con la finalidad de evitar la amplificación de los efectos lesivos de la conducta ilícita.

Pero, pese a estos avances, la necesidad de desarrollo legislativo sigue latente a medida que el progreso técnico da lugar a nuevas situaciones que requieren respuestas de carácter penal-sancionador. Por ello, el legislador europeo está promoviendo nuevos proyectos para impulsar esa misma armonización normativa en otros ámbitos también afectados por el carácter transnacional del fenómeno. Tal es el caso de la nueva Directiva sobre servicios de pago (PSD3), que sustituirá a la actual Directiva (UE) 2015/2366, y del Reglamento sobre servicios de pago (PSR), cuya incidencia, al menos indirecta, en la ciberdelincuencia parece evidente, ya que uno de sus objetivos es combatir el fraude en los pagos digitales, fortalecer la seguridad y mejorar la protección de los usuarios de los servicios de pago, particularmente en las operaciones *online*.

Igualmente, en los últimos años se vienen multiplicando los esfuerzos para mejorar la protección de niños, niñas y adolescentes en el entorno digital. La preocupación por las agresiones sexuales a menores, tanto en el entorno físico como virtual, dio lugar al planteamiento de la Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores, con el fin de impulsar la erradicación progresiva de estas graves y peligrosas conductas.

En el marco de esta Estrategia se encuadran los trabajos en curso, impulsados entre los años 2020 y 2025, para actualizar las herramientas legales contra el abuso sexual de menores que, además de la adecuación de la Directiva (UE) 2011/93, antes citada, incluyen otras iniciativas orientadas a incentivar y reforzar la cooperación policial y judicial internacional en ese tipo de investigaciones, mejorar la protección de las víctimas y fomentar la sensibilización social y la denuncia sobre CSAM [18]. Se trata, en definitiva, de ofrecer una respuesta eficaz frente a las nuevas formas de agresión que han ido surgiendo

[18] Son las siglas de la expresión *Child Sexual Abuse Material*, con la que se pretende sustituir a nivel internacional la referencia a pornografía infantil, en el entendimiento de que este

con los avances técnicos y científicos y las posibilidades de acción que ofrecen los sistemas IA (particularmente en lo relativo a la elaboración de CSAM ultrafalsificado), propiciando al tiempo la persecución y sanción de los responsables de estos delitos. Al hilo de esta Estrategia, también se están realizando innegables esfuerzos a nivel comunitario para la elaboración de un Reglamento sobre adopción de medidas para la detección, denuncia y eliminación de CSAM en el entorno virtual, actuación que sería apoyada por un nuevo organismo articulado específicamente para ello, el Centro de la UE sobre Abuso Sexual de Menores.

Finalmente, en este rápido repaso a la normativa actualmente vigente, no podemos omitir una referencia expresa al conocido como paquete *e-evidence* –Reglamento (UE) 2023/1543 y Directiva (UE) 2023/1544, ambos de 12 de julio– que será de aplicación plena este mismo año 2026, con el que se pretende establecer un régimen ágil y sencillo de colaboración entre las autoridades de los Estados miembros de la Unión y los prestadores de servicio establecidos en el territorio comunitario para la obtención transnacional de evidencias mediante órdenes europeas de producción y de conservación de pruebas electrónicas en procesos penales y de ejecución de penas privativas de libertad.

Con todo, ha de recordarse que la preocupación por los gravísimos efectos que el uso irregular de las TIC está produciendo en la delincuencia transciende al ámbito UE y alcanza a la comunidad universal. Buen ejemplo de ello fue la publicación por el Consejo de Europa (CoE), en noviembre de 2001, del Convenio de Budapest sobre Ciberdelincuencia, del que actualmente forman parte 81 Estados de todos los marcos geográficos y que ha sido –y sigue siendo– el principal motor de la intensa armonización normativa en esta materia. Precisamente dicho Convenio se ha visto reforzado con la apertura a la firma en mayo de 2022 de su Segundo Protocolo Adicional dedicado a promover y potenciar la cooperación y mejorar la obtención de pruebas electrónicas entre los distintos países miembros. También es reflejo de esa misma preocupación la aprobación por la Asamblea General de las Naciones Unidas a finales del año 2024 de la Convención contra la Ciberdelincuencia y para el fortalecimiento de la Cooperación Internacional para la lucha contra determinados delitos cometidos mediante sistemas de tecnología de la información y la comunicación y para la transmisión de pruebas en forma electrónica de delitos graves, inspi-

---

tipo de material procede siempre de actos de abuso/agresión sexual sobre menores que no tienen capacidad de consentimiento.

rada en gran medida en el Convenio de Budapest, si bien en este caso con proyección universal. Dicho documento se abrió a la firma en Hanoi (Vietnam) en octubre del pasado año 2025, habiéndose firmado por más de 70 Estados.

En nuestro país, siguiendo ese mismo planteamiento, también se está trabajando intensamente desde hace varias décadas para garantizar la seguridad en el ciberespacio y dotar a operadores jurídicos e investigadores de las herramientas necesarias para defender a los ciudadanos y las ciudadanas frente a la ciberdelincuencia. Sin pretensión de exhaustividad no pueden dejar de mencionarse la Estrategia Nacional de Ciberseguridad de 2019; el Esquema Nacional de Seguridad, aprobado por RD 311/2022, de 3 de mayo; el Real Decreto-ley 12/2018, de 7 de septiembre, *de seguridad de las redes y sistemas de información*, que implementa en el ordenamiento jurídico interno la Directiva (UE) 2016/1148 *–Directiva NIS 1–*, o la Ley 8/2011, de 28 de abril, *por la que se establecen medidas para la protección de las infraestructuras críticas*, así como la articulación de diversos organismos como el Instituto Nacional de Ciberseguridad (INCIBE), la Oficina de Coordinación en Ciberseguridad (OCC) y más recientemente la creación de la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA), mediante Real Decreto 729/2023. Además, han de citarse las profundas reformas que se vienen realizando en el Código Penal y en la Ley de Enjuiciamiento Criminal para adecuar nuestras herramientas legales a las nuevas formas de agresión a bienes jurídicos susceptibles de protección penal.

Al igual que en el ámbito internacional, el legislador nacional se ve constantemente impelido a abordar nuevos proyectos para responder a las inéditas situaciones que constantemente se van generando. A ello responden el Plan Nacional de Ciberseguridad, aprobado en 2022, o el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, pendiente de remisión al Parlamento, con el que se pretende transponer en la normativa interna la Directiva (UE) 2022/2555 –Directiva NIS 2– y en el que se reconoce un importante papel al Ministerio Fiscal a efectos de hacer posible una adecuada coordinación entre la acción preventiva y la acción sancionadora del Estado frente a los ataques informáticos. También ha de mencionarse en este apartado la aprobación por el Gobierno de España, en el mes de marzo del pasado año 2025, del Anteproyecto de Ley para el Buen Uso y la Gobernanza de la Inteligencia Artificial.

Por otra parte, el interés en salvaguardar a los más vulnerables frente al uso irregular del ciberespacio se ha concretado en el Proyecto de Ley Orgánica para la protección de las personas menores de

edad en los entornos digitales. En dicho texto, fruto del trabajo colectivo de distintos organismos e instituciones, así como de entidades del sector privado, se aborda una ambiciosa propuesta con la que se pretende garantizar los derechos e intereses de niños, niñas y adolescentes en el ciberespacio y ayudarles y orientarles en el uso responsable de las tecnologías tanto en sus relaciones personales como en los diversos aspectos de su formación, desarrollo y evolución. Por ello, en el Proyecto, además de una declaración expresa de los derechos que corresponden *online* a la infancia y adolescencia, se incluyen previsiones para mejorar la atención y cuidado de los menores en aspectos de carácter educativo y sanitario y también propuestas de reforma de algunos textos legales como la Ley Orgánica 3/2018, de 5 de diciembre, *de Protección de Datos Personales y garantía de los derechos digitales* –a fin de elevar a 16 años la edad para consentir la cesión de datos personales–, la Ley General de Comunicación Audiovisual, la Ley de Enjuiciamiento Criminal o la Ley Orgánica del Poder Judicial. Entre estas novedades merece especial mención la modificación de determinados preceptos del Código Penal para mejorar la medidas preventivas y sancionatorias frente a las agresiones *online* respecto de menores de edad, particularmente las que afectan a su libertad sexual, así como la incorporación de un nuevo delito que castiga la transmisión y/o difusión a terceros de *deepfakes* de carácter sexual o vejatorio que atenten contra la integridad moral de personas concretas e identificadas.

También se encuentra en trámite en nuestro país la adecuación de la legislación a la normativa *e-evidence*, antes citada, Reglamento (UE) 2023/1543 y Directiva (UE) 2023/1544, cuya aplicación efectiva va a ser de especial trascendencia para mejorar y agilizar la conservación y obtención transnacional de evidencias electrónicas en las investigaciones y procesos penales y, por ende, la actuación frente a la ciberdelincuencia en el territorio comunitario.