8. Criminalidad informática

8.1 **Introducción**

El día 26 de diciembre del pasado año 2024 la Asamblea General de las Naciones Unidas (en adelante, NNUU) adoptaba el texto 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», inspirada, en gran medida, en el Convenio de Budapest del Consejo de Europa (en adelante, CoE) del año 2001. Esta nueva Convención es el resultado de un esfuerzo colectivo empeñado por los Estados Miembros de NNUU, junto con instituciones académicas del sector privado y la sociedad civil, que se ha desarrollado durante los últimos cinco años y ha culminado con la preparación del borrador, inicialmente aprobado en agosto del pasado año. El objetivo del documento, como su propio nombre indica, es prevenir y combatir la ciberdelincuencia de la manera más eficiente y eficaz mediante la articulación de herramientas legales adecuadas, el fortalecimiento de la cooperación internacional y la prestación de asistencia técnica y apoyo para la creación de capacidades, especialmente en los Estados en desarrollo.

Al margen de las reticencias que este documento ha generado en muchos países, y también en organizaciones de derechos humanos y de defensa de los derechos digitales, debido al riesgo –especialmente grave en regímenes autoritarios– de que bajo la cobertura de una supuesta actuación frente a la ciberdelincuencia se encubran graves restricciones a la libertad de expresión, de información y otras libertades y derechos fundamentales de las personas, la Convención constituye un excelente indicador de la creciente preocupación mundial ante el incremento, cuantitativo y cualitativo, de la delincuencia en el entorno virtual en los últimos años. Dicha progresión se ha visto favorecida por los constantes avances técnicos y científicos, las posibilidades que ofrece la encriptación y otros sistemas de anonimización y el aumento de las capacidades de actuación en el ciberespacio, extraordinariamente potenciadas en los últimos años por el recurso a los sistemas de inteligencia artificial (IA).

La necesidad de proteger la resiliencia y seguridad de redes y sistemas informáticos frente al uso irregular y/o delictivo de estas tecnologías, claramente perceptible desde hace varios años, viene marcando la agenda legislativa de los Estados en los distintos marcos geográfi-

cos desde principios de este siglo, tanto en los aspectos preventivos como de investigación y persecución penal, impulsando al tiempo la cooperación internacional en uno y otro plano. La gran aportación del Convenio de Budapest en este proceso y en particular en los aspectos relacionados con la lucha contra la ciberdelincuencia resulta incuestionable. La regulación que se recoge en su capítulo II, acerca de la definición de conductas delictivas y también de medidas de investigación criminal, ha inspirado y sigue haciéndolo la normativa interna de un buen número de países de los cinco continentes y está en el origen de muchas de las previsiones que se contemplan en la Convención de NNUU antes citada, pues no en vano 76 países del mundo pertenecientes a los cinco continentes son actualmente miembros del citado Convenio del CoE.

Esta influencia ha sido particularmente intensa en el desarrollo normativo que se ha llevado a efecto en el marco comunitario, especialmente a partir del Consejo de la Unión Europea (en adelante UE) de noviembre de 2008 en el que se acordó tomar como referencia para la lucha contra la ciberdelincuencia las directrices del Convenio de Budapest. Buena muestra de ello son, entre otras, la Directivas (UE) 2013/40 de 12 de agosto, relativa a los ataques contra los sistemas de información, la Directiva (UE) 2011/93 de 13 de diciembre relativa a la lucha contra los abusos sexuales, la explotación sexual de los menores y la pornografía infantil, que se inspira también en el Convenio de Lanzarote del CoE de 2007, y también, en cierta medida, la Directiva (UE) 2019/713 de 17 de abril, sobre lucha la contra el fraude y falsificación de medios de pago distintos del efectivo, incorporada al ordenamiento jurídico español por Ley Orgánica 14/2022, de 22 de diciembre. La influencia del Convenio de Budapest ha sido especialmente intensa en los Estados miembros de la UE también en los aspectos procesales o de investigación criminal y su efecto se ha dejado notar claramente en nuestro país con la reforma operada por Ley Orgánica 13/2015, de 5 de octubre, que incorpora en nuestra añeja Ley de Enjuiciamiento Criminal (en adelante, LECrim) las herramientas de investigación tecnológica.

No obstante, los avances científicos y técnicos junto a la profunda digitalización de nuestra sociedad en los últimos años, en buena medida impulsada por las especiales circunstancias generadas con ocasión de la pandemia, nos enfrenta constantemente a nuevos retos y desafíos que es necesario abordar para garantizar el pleno ejercicio de los derechos y libertades de las personas en el entorno virtual y, en definitiva, la seguridad en el ciberespacio. El alto nivel de conectividad entre las personas, organismos e instituciones, el carácter transnacional de las

actividades *online*, la potencialidad de los sistemas de inteligencia artificial, el crecimiento exponencial del comercio electrónico y la economía digital, en ocasiones vinculada al uso de criptoactivos, sin duda alguna aportan grandes ventajas y oportunidades para la evolución de los pueblos y el desarrollo y progreso de la humanidad, pero también pueden generar efectos perversos si se utilizan de forma inadecuada o con finalidades ilícitas. La plena conciencia de esta situación está dando lugar a un intenso proceso de elaboración normativa, a nivel nacional e internacional, con el objetivo de aprovechar al máximo estas potencialidades y, al tiempo, proteger a la ciudadanía de los efectos perversos que de ello pudieran derivarse. En definitiva, lo que se pretende es mejorar la seguridad y resiliencia de redes y sistemas informáticos, prevenir la actividad irregular y/o delictiva en la red y potenciar y reforzar nuestra capacidad de investigación, persecución y sanción de las acciones ilícitas que se planifican y/o ejecutan en el ciberespacio.

Al analizar la actuación regulatoria en el ámbito de la prevención en el último periodo anual es de mención obligada la aprobación por el Consejo de Ministros, en los primeros días del presente año 2025, del Anteproyecto de Ley sobre Coordinación y Gobernanza de Ciberseguridad, con el que se pretende transponer en la normativa interna la Directiva (UE) 2022/2555 sobre seguridad de las redes y sistemas de información. Esta disposición europea, conocida como directiva NIS 2, define un marco actualizado en el espacio comunitario para la prevención, detección temprana y gestión de ciberamenazas, con el objetivo de reforzar los mecanismos para la protección y resiliencia de las redes y sistemas informáticos, ya establecido en la Directiva (UE) 2016/118 de 6 de julio (Directiva NIS1), que fue incorporada al ordenamiento jurídico español por el Real Decreto-ley 12/2018, de 7 de septiembre. De acuerdo con esos mismos objetivos, el Anteproyecto de Ley en tramitación pretende la puesta en funcionamiento de un Centro Nacional de Ciberseguridad como organismo encargado de la coordinación de toda esta materia a nivel nacional.

Otro hito importante en esta materia ha sido la entrada en vigor, en diciembre de 2024, de la Ley Europea de Ciberresiliencia (CRA) –Reglamento (UE) 2024/2847 de 23 de octubre– por la que se establecen requisitos obligatorios de ciberseguridad en los productos con elementos digitales para garantizar de forma más completa y efectiva la seguridad de los consumidores, particularmente de aquellos que por sus circunstancias son más vulnerables.

Precisamente, el irrenunciable propósito de cohonestar el aprovechamiento de los avances técnicos y científicos con los valores esenciales de la Unión, la protección de la salud, la seguridad y los derechos de todos, está igualmente en el origen de la preparación y elaboración del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo sobre Inteligencia Artificial, publicado el 13 de junio del pasado año. Siguiendo las directrices del citado Reglamento, en los primeros meses del presente año 2025 se ha iniciado en España la elaboración de un proyecto de ley sobre gobernanza de la IA en el que, entre otros aspectos, se establecen los criterios para su correcta utilización así como las autoridades encargadas de vigilar la utilización adecuada de los sistemas de alto riesgo y la no aplicación de los prohibidos, y en el que se propone atribuir estas funciones al Consejo General del Poder Judicial en el ámbito de la Justicia.

Por otra parte, y ya en referencia a la lucha contra la ciberdelincuencia, la necesidad de articular herramientas legales que hagan posible una respuesta penal efectiva frente a las nuevas formas de agresión contra bienes jurídicos de carácter personalísimo determinó la publicación el pasado año de la Directiva (UE) 2024/1385 del Parlamento Europeo y del Consejo, de 14 de mayo, sobre la lucha contra la violencia contra las mujeres y la violencia doméstica. Esta disposición, en sus artículos 5 a 9, define como delitos determinados comportamientos *online* que atentan contra dichos bienes jurídicos, tales como la difusión no consentida de material íntimo o manipulado artificialmente, el ciberacecho, como forma de vigilancia electrónica no autorizada, el ciberacoso *(cyber harassment),* el ciberexhibicionismo *(cyber flashing)* o la incitación a la violencia y al odio por medios cibernéticos. Con ello se trata de proteger a las niñas y mujeres, además de a otras posibles víctimas, frente a actos de violencia vinculados al uso de las TIC y también del riesgo de difusión masiva de contenidos que atentan contra su intimidad, su libertad o su dignidad, evitando de esta forma la amplificación de los efectos lesivos de la conducta ilícita. Con ese mismo objetivo, en el marco de la Estrategia Europea contra el abuso sexual infantil para el quinquenio 2020-2025, se iniciaron en 2023 los trabajos en curso para la modificación de la Directiva (UE) 2011/93 del Parlamento europeo y del Consejo de 13 de diciembre, contra el abuso sexual de menores. La reforma de este texto pretende adecuar la definición de las conductas delictivas a las formas de abuso y explotación sexual de personas menores, facilitadas por los avances técnicos y las capacidades de acción de los sistemas IA –como acontece con la elaboración de material de abuso sexual infantil (en adelante, CSAM) ultra falsificado–, así como

mejorar las herramientas legales para la investigación de estos comportamientos y al tiempo propiciar una mejor y más efectiva coordinación en la prevención de estas conductas, la protección de las víctimas y la lucha eficaz contra estas manifestaciones criminales.

Pero, como ya se ha indicado, la respuesta eficaz frente a estas novedosas agresiones no solo precisa de la definición de conductas delictivas hasta ahora inéditas, o de la adecuación de las ya existentes a formas de comisión no previstas, sino que también es imprescindible la articulación de herramientas legales que contribuyan a mejorar las posibilidades de investigación de estos graves ilícitos y de identificación de sus responsables. A ello responde el proyecto de Reglamento sobre el que se está trabajando actualmente en la Unión Europea con el objetivo de definir en el marco comunitario medidas que faciliten la detección de contenidos CSAM en el entono virtual, materia regulada actualmente con carácter provisional por el Reglamento (UE) 2024/1307 de 29 de abril, que excepciona temporalmente la aplicación de determinadas disposiciones de la Directiva 2002/58/CE de 12 de julio, sobre privacidad en las comunicaciones, que impedirían la utilización de determinadas técnicas de rastreo y localización empleadas habitualmente con dicho objetivo.

También, con la finalidad de proteger a las víctimas y evitar que la difusión de contenidos que atentan contra sus derechos y libertades amplifique los efectos perversos de estas conductas, tanto la Directiva (UE) 2024/1385, en su artículo 23, como la Directiva (UE) 2011/93, en su artículo 30, contemplan medidas orientadas a garantizar su retirada del entono virtual. Igualmente, el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre, sobre servicios digitales, en vigor desde el 17 de febrero del pasado año 2024, refuerza ese mismo marco de protección estableciendo concretas obligaciones para los prestadores de servicios digitales referidas, en lo que aquí interesa, al cumplimiento de las órdenes de actuación emitidas por las autoridades judiciales o administrativas respecto de contenidos ilícitos (art. 9) y al establecimiento de medidas específicas para la protección de los menores en línea (art. 28).

Esta misma preocupación por salvaguardar los intereses de los más vulnerables frente a un uso irregular del ciberespacio ha determinado en nuestro país la remisión a las Cortes Generales, en marzo del presente año 2025, de un proyecto de ley orgánica para la protección integral de las personas menores de edad en los entornos digitales. En este documento, fruto del trabajo de un nutrido grupo de expertos de distintas disciplinas y de las aportaciones de diversas instituciones, que en el momento de elaborar esta Memoria inicia su andadura parla-

mentaria, se recogen una pluralidad de propuestas orientadas a garantizar los derechos e intereses de los y las niños, niñas y adolescentes y a favorecer el uso responsable de las tecnologías por dicho colectivo en los diversos ámbitos de actividad *online* en que canalizan su formación, aficiones, acciones de interés personal y esparcimiento y, en definitiva, sus relaciones con los demás. Entre dichas previsiones se incluyen medidas de protección en los sectores educativo y sanitario, junto a propuestas de modificación de importantes disposiciones legales tales como la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de Derechos Digitales, para elevar a los 16 años la edad para consentir la cesión de datos personales, la Ley de Enjuiciamiento Criminal, la Ley Orgánica del Poder Judicial, así como también el Código Penal. En este último se incorporan algunas novedades de especial interés, orientadas tanto a reforzar la protección de los menores de edad frente a las agresiones de las que son víctimas en el ciberespacio, particularmente las que afectan a su libertad sexual, como a prevenir la reiteración de dichos comportamientos.

Finalmente, en este sucinto repaso de los avances normativos en la materia que nos ocupa, no podemos omitir una breve referencia a los trabajos en curso para la adecuación de la legislación interna al paquete normativo *e-evidence* Reglamento (UE) 2023/1543 y Directiva (UE) 2023/1544, ambas de 12 de julio, y a los múltiples estudios y reflexiones que se están realizando en el seno de las diversas áreas de especialización del Ministerio Fiscal acerca de las órdenes europeas de producción y de conservación de pruebas electrónicas en los procesos penales y de ejecución de penas privativas de libertad, cuya contribución a una actuación coordinada contra la ciberdelincuencia en el marco comunitario resulta incuestionable.

Igualmente ha de ponerse de manifiesto nuestro empeño en una pronta ratificación del Segundo Protocolo Adicional al Convenio de Budapest, abierto a la firma el 12 de mayo de 2022 y suscrito por España en esa misma fecha, que también tiene el objetivo de favorecer y facilitar la obtención transnacional de evidencias electrónicas con fines de investigación criminal en un marco mucho más amplio y abierto que el anterior, pues su futura aplicación se proyecta más allá del territorio de la UE. El valor de este documento para nuestro país resulta esencial a efectos de potenciar y canalizar nuestra cooperación frente a la ciberdelincuencia con las autoridades competentes de los países de habla hispana con las que, por utilizar una lengua común, hemos de colaborar en múltiples y diversas investigaciones relacionadas con ciberdelitos. No en vano un número significativo de países latinoamericanos –Argentina, Chile, Colombia, Costa Rica, Ecuador,

Panamá, Paraguay, Perú y República Dominicana–, son en la actualidad miembros del citado Convenio internacional y algunos otros, como Uruguay, se encuentran próximos a suscribirlo.