8. CRIMINALIDAD INFORMATICA

8.1 **Introducción**

Un año más hemos de llamar la atención sobre la extraordinaria incidencia que el imparable desarrollo tecnológico está teniendo en el desenvolvimiento de la sociedad, en el funcionamiento de las instituciones, en el de los organismos públicos, privados y en la actividad de todos/as los ciudadanos/as del mundo.

Los avances en el ámbito científico y técnico; el uso cada vez más frecuente de medios digitales y servicios en la nube; la complejidad e interconexión de los sistemas informáticos; o el trabajo a distancia son factores que están influyendo en el planteamiento y organización estructural de todo tipo de grupos sociales y comunidades cualquiera que sea su naturaleza, fines u objetivos e incluso en el funcionamiento de los Estados, al tiempo que generan un imparable y beneficioso impulso de la economía digital y del comercio electrónico.

Esta creciente digitalización está teniendo también un evidente reflejo en nuestra forma de relacionarnos con los demás en los múltiples y diversos ámbitos en que nos desarrollamos como personas –familiar, profesional, económico o social– e incidiendo, sin duda, en la perspectiva con la que cada uno de los seres humanos observamos y abordamos nuestra propia existencia.

Es innegable que la penetración de las tecnologías en la cotidianeidad de los/as ciudadanos es cada vez más intensa y nos enfrenta a serios desafíos que afectan a aspectos esenciales del ser humano y que como sociedad hemos de afrontar conjuntamente. No en vano el nivel de conectividad que hemos alcanzado ha ido difuminando, en cierta medida los rígidos y estrictos límites fronterizos de los Estados, a consecuencia del traslado de muchos aspectos de nuestra actividad diaria a un ciberespacio en el que claramente percibimos nuestra condición de habitantes del mundo. Por ello, en el marco internacional son cada vez más intensos y profundos los esfuerzos para articular conjuntamente parámetros de convergencia y principios de acuerdo, al menos en los aspectos esenciales, que hagan posible cohonestar el aprovechamiento óptimo de las grandes ventajas que ofrecen las tecnologías para el progreso de la humanidad con el pleno respeto de los derechos y libertades individuales y de las garantías y valores inherentes a las sociedades libres y democráticas.

El Preámbulo de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre Inteligencia Artificial, cuyo texto ha quedado definitivamente fijado el 9 de diciembre del pasado año 2023

por acuerdo del Parlamento y del Consejo de la UE, es fiel reflejo de este planteamiento al dejar clara constancia del amplio abanico de beneficios que dichas tecnologías de rápida evolución pueden aportar en todos los sectores y actividades sociales –salud de las personas, medio ambiente, cambio climático, finanzas, movilidad social–, pero también de los riesgos o consecuencias negativas que su uso inadecuado puede entrañar para individuos aislados o para la sociedad en su conjunto. Por ello, y a partir de *un enfoque europeo coordinado sobre las implicaciones éticas y humanas de la IA,* la Propuesta de Reglamento apuesta por un planteamiento equilibrado con el que se pretende garantizar *que los europeos puedan aprovechar nuevas tecnologías que se desarrollen y funcionen de acuerdo con los valores, los derechos fundamentales y los principios de la UE.*

Es éste solo un ejemplo –aunque de incuestionable interés por su extraordinario alcance e implicaciones en todas las áreas de la actividad humana– del esfuerzo titánico que se viene desarrollando desde hace años en los distintos marcos geográficos para ofrecer respuestas efectivas y eficaces ante la necesidad cada vez más acuciante de hacer posible un uso seguro del ciberespacio frente a las crecientes amenazas que ponen en riesgo el funcionamiento de organismos e instituciones e incluso el pleno ejercicio de los derechos y libertades públicas. Con ese objetivo se está avanzando en los múltiples ámbitos que se ven afectados por la capilarización tecnológica de las relaciones interpersonales en todas sus manifestaciones pues, no en vano, ciberseguridad; ciberdefensa; ciberdiplomacia; ciberfinanzas y economía digital o ciberdelincuencia, no son sino aspectos distintos, aunque relacionados entre sí, de una misma problemática que ha de abordarse a partir de un planteamiento conjunto e integrador.

Así, el esfuerzo desarrollado en años anteriores para reforzar la seguridad de redes y sistemas informáticos en sectores vitales para la sociedad y la economía comunitarias, que culminó a finales de 2022 con la publicación de la Directiva (UE) 2022/2555 *sobre medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión* –también conocida como Directiva NIS2– así como de la Directiva (UE) 2022/2557 *sobre resiliencia de entidades críticas* y del Reglamento (UE) 2022/2554 *sobre resiliencia operativa digital*, centrado en el sector financiero, se ha visto complementado en el año 2023 con la publicación en el DOUE del Reglamento (UE) 2023/2841 de 13 de diciembre, en el que se establecen medidas comunes de ciberseguridad para las propias instituciones, órganos y organismos de la Unión Europea.

Siguiendo ese mismo planteamiento, en la actualidad se encuentra en elaboración un Reglamento sobre Ciberesiliencia con el que se pretende garantizar, a ciudadanos y empresas, la seguridad de los productos digitales que se pongan a su disposición, a cuyo fin se establecerán por diseño requisitos de ciberseguridad obligatorios en el territorio comunitario para todos los dispositivos y sistemas de información. Los importantes avances en la preparación de este último documento han determinado que el Parlamento y el Consejo alcanzaran el necesario acuerdo sobre su contenido el 30 de noviembre del pasado 2023.

Mas directamente relacionado con la materia que nos ocupa, ha de mencionarse el Reglamento (UE) 2022/2065 de 19 de octubre *relativo al mercado único de servicios digitales,* cuyo objetivo principal, además de articular las normas de competencia entre las empresas del sector, es el de garantizar la seguridad de los usuarios y consumidores *online* a partir de un marco regulatorio en el que se fijan con claridad las obligaciones que corresponden a los distintos servicios de la sociedad de la información, como mercados en línea, redes sociales o plataformas de intercambio de contenidos, tanto en los aspectos relacionados con la transparencia de sus operaciones como en lo relativo al cumplimiento de las medidas establecidas en garantía de los derechos de los usuarios y de las ordenes emanadas de las autoridades competentes. Entre ellas, y en lo que aquí interesa, las relativas a la retirada de contenidos ilícitos (art.9) o a la entrega de información (art.10) dictadas por las autoridades judiciales o administrativas en el ejercicio de sus competencias, o también las obligaciones establecidas sobre notificación de sospechas acerca de la comisión de ilícitos penales o las orientadas a la protección en línea de los menores de edad (art.28). Dicho Reglamento se encuentra en vigor desde el 17 de febrero del presente año 2024, habiéndose atribuido a la Comisión Nacional de los Mercados y de la Competencia (CNMC) la función de Coordinador de Servicios Digitales en orden a su aplicación y ejecución en nuestro país.

Precisamente, una de las más graves consecuencias del uso irregular del ciberespacio es su incidencia en el ámbito de la delincuencia, circunstancia de la que claramente se deja constancia en nuestra Estrategia Nacional de Ciberseguridad de 2019 y también en la Estrategia de Ciberseguridad de la UE para la década digital, publicada el 10 de junio del 2021. Por ello, desde principios de este milenio se viene trabajando en el ámbito interno e internacional para articular herramientas legales que permitan actuar de forma efectiva y con sujeción plena a las garantías inherentes al Estado de Derecho frente a un fenómeno criminal, especialmente peligroso y grave, que evoluciona vertigino-

samente al hilo del desarrollo tecnológico afectando a bienes jurídicos de muy diversa naturaleza y expandiéndose sin sujeción alguna a las fronteras y límites territoriales de los Estados.

Ya hemos dado cuenta en anteriores Memorias de los importantes avances legislativos que se han ido realizando en los distintos marcos geográficos a fin de articular, sobre la base de una progresiva aproximación de los ordenamientos jurídicos internos, herramientas legales comunes para mejorar la capacidad de actuación y respuesta frente a estos fenómenos criminales. Los esfuerzos realizados en esa dirección en el ámbito comunitario son sin duda destacables. En este año memorial hemos de reseñar, entre otros, el impulso dado a la Propuesta de Directiva del Parlamento Europeo y del Consejo *sobre lucha contra la violencia sobre las mujeres y violencia doméstica,* respecto de la cual se ha logrado el acuerdo de aprobación por ambas instituciones comunitarias en los primeros días de febrero del presente año 2024. En dicha disposición normativa se aborda específicamente la ciberviolencia contra las mujeres, cuyo incremento, vinculado al progreso tecnológico y a la profunda digitalización de nuestra sociedad, es claramente perceptible y, en definitiva, constituye la prolongación *online* de la misma lacra que venimos sufriendo con tan graves consecuencias en el entorno físico. La carencias en el tratamiento de esta materia en los textos internacionales vigentes se subsanan, al menos parcialmente, con la definición como delitos de determinadas conductas que habitualmente se planifican y ejecutan *online*, tales como la difusión no consentida de material íntimo o manipulado (art.7), el ciberacecho en sus diversas manifestaciones –entre ellas la vigilancia a través de medios electrónicos– (art. 8), las conductas de ciberacoso (art.9) y las relacionadas con el discurso de odio por razones de sexo o género (art.10) y también con la referencia expresa en el art. 25 a medidas orientadas a evitar la accesibilidad de contenidos ilícitos de esta naturaleza.

Pero, además, el año 2024 nos ha sorprendido con la propuesta de la Comisión Europea, publicada el día 6 de febrero, de modificación de la Directiva (UE) 2011/93 *relativa a la lucha contra los abusos sexuales, la explotación sexual de los menores y la pornografía infantil.* Una modificación que se enmarca en el desarrollo de la Estrategia de la Unión Europea para una lucha más eficaz contra el abuso sexual de menores, presentada por la Comisión en julio del año 2020 con la finalidad de establecer nuevas herramientas legales o adecuar las ya previstas a las necesidades de reforzar y hacer más efectiva la respuesta penal frente a las nuevas formas de ataque a la libertad sexual de los menores que han ido surgiendo vinculadas a los avances científ-

ficos y técnicos, particularmente las que se sirven de sistemas de inteligencia artificial con dichas finalidades ilícitas.

La preocupación que existe en amplios sectores sociales acerca de los riesgos y amenazas a los que se enfrentan los más jóvenes en la red ha determinado que nuestro país se haya implicado muy directamente en este proyecto, cuya conexión con la iniciativa legislativa sobre violencia contra la mujer es más que evidente pues, como se indica en el Preámbulo de dicha Directiva, la coincidencia temporal de ambos trabajos *ofrece la oportunidad de garantizar la coherencia global del marco específico para proteger a los menores contra todas las formas de abuso sexual y de explotación sexual*.

Pero, como ya hemos indicado, la actuación eficaz frente a estos ilícitos comportamientos exige necesariamente reforzar la cooperación entre las autoridades policiales y judiciales de los distintos países y también con las entidades del sector privado que intervienen como intermediarios en los procesos de comunicación a través de los cuales se planifican y ejecutan las actividades delictivas. Son también destacables los esfuerzos que se vienen realizando en los últimos años con ese objetivo. En el marco comunitario el hito más significativo ha sido, sin duda, la publicación en el DOUE de 28 de julio de 2023 del conocido como *paquete e-evidence* –Reglamento (UE) 2023/1543 y Directiva (UE) 2023/1544– sobre prueba electrónica en procesos penales, cuya importancia a efectos de la investigación y enjuiciamiento de los ciberdelitos es incuestionable pues va a facilitar notablemente la obtención, mediante petición directa a los propios proveedores de servicios, de aquellas evidencias electrónicas almacenadas en otros Estados miembros –datos de abonado, tráfico o contenido– que resulten imprescindibles para el éxito de las actuaciones penales relativas a ilícitos ejecutados en el ciberespacio. Precisamente, la trascendencia de estos documentos en orden a mejorar nuestra capacidad de acción frente la ciberdelincuencia ha determinado el inicio, tanto en nuestro país como en el ámbito comunitario, de los trabajos preparatorios para hacer posible que la adecuación de las legislaciones internas a esta normativa sea lo más armónica posible, de forma que se garantice el uso ágil y efectivo de estas nuevas herramientas de cooperación en todo el territorio UE.

Igual propósito de favorecer la obtención transnacional de pruebas electrónicas, aunque en referencia a un marco geográfico más abierto, ha impulsado la elaboración del Segundo Protocolo Adicional a la Convención de Budapest sobre Ciberdelincuencia del Consejo de Europa *relativo a la cooperación reforzada y la revelación de pruebas electrónicas* que se abrió a la firma de los Estados Miembro en mayo

de 2022. El Consejo de la Unión Europea, por Decisión (UE) 2023/436 de 14 de febrero, ha autorizado a los Estados del marco comunitario a ratificar dicho Protocolo Adicional que ya ha sido firmado por 41 países de los que dos, Serbia y Japón, lo han ratificado. También en este caso, la entrada en vigor de este Tratado, que exige la ratificación como mínimo de 5 miembros, contribuirá a mejorar ostensiblemente la investigación y actuación penal frente a ilícitos *online* de carácter transnacional y, particularmente en el caso de España, la colaboración con las autoridades judiciales y policiales de los países de la comunidad iberoamericana para la investigación y enjuiciamiento de las actividades ilícitas *online* que se cometen en nuestra lengua común.

Finalmente, si bien con proyección universal, es obligada la mención a los trabajos que, aun con ciertas dificultades, se siguen manteniendo en el marco de NN.UU para la elaboración de la denominada *Convención Internacional Integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos,* cuyo objetivo es aproximar las legislaciones internas de los Estados en la definición de tipos penales y de herramientas de investigación criminal y establecer medidas para mejorar la cooperación transnacional frente a la ciberdelincuencia.