8. CRIMINALIDAD INFORMÁTICA

8.1 **Introducción**

La intensa penetración de las tecnologías de la información y la comunicación, en adelante TIC, en todos los aspectos de las relaciones entre las personas sigue marcando, como en años precedentes, la actividad económica, política y social, las líneas de acción de los Estados en los cinco continentes y el desarrollo y evolución de la humanidad en su conjunto. La Internet de las cosas, la implantación definitiva del 5G, la inteligencia artificial o los ordenadores cuánticos nos proyectan hacia un futuro solo parcialmente imaginable que, sin duda, aportará grandes ventajas y beneficios para los ciudadanos/as pero que también generará nuevos riesgos y amenazas para la seguridad de todos y todas e incluso para el pleno ejercicio de los derechos y libertades que nos corresponden como personas, si dichos avances no vienen acompañados de las medidas necesarias para garantizar un uso seguro del ciberespacio.

Precisamente uno de los efectos perversos que se están derivando de esta evolución tecnológica es el aprovechamiento de las TIC con finalidades criminales, circunstancia que está generando un claro desplazamiento de la actividad delictiva al entono virtual. Así es significativo que el último informe sobre evolución de la delincuencia en España publicado el mes de marzo del presente año 2023 por el Ministerio del Interior cifre en el 16,1% la incidencia de la ciberdelincuencia en el conjunto de la actividad delictiva en nuestro país, lo que implica un incremento en más de 6 puntos respecto del índice del 9,9% obtenido por igual concepto en el año 2019 y es reflejo del crecimiento en un 72% en el volumen de ilícitos de esta naturaleza entre ambos periodos anuales. A ello responde igualmente la preocupación generada a nivel mundial por la gravedad y frecuencia de los ataques de *ransomware,* particularmente en los sectores sanitario, financiero y educativo o de los ataques a IoT *(the internet of Things)* y también por la progresiva utilización de criptomonedas u otros instrumentos de pago distintos del efectivo con objetivos fraudulentos, actuaciones criminales que en uno y otro caso están generando cuantiosísimos perjuicios económicos. Ello sin olvidar el peligroso repunte constatado a nivel mundial en las agresiones *online* contra bienes jurídicos especialmente sensibles como la libertad sexual de los menores.

Conscientes de esta realidad, en el pasado año 2022, los poderes públicos de todos los Estados del mundo, en particular los de nuestro entorno más próximo y también las organizaciones internacionales

con responsabilidad en esta materia han seguido trabajando para promover y adoptar conjuntamente líneas de acción que hagan posible cohonestar el aprovechamiento efectivo de las extraordinarias posibilidades de acción que ofrecen las TIC para el progreso de la humanidad con la adopción de normas básicas, comúnmente aceptadas, que garanticen el uso seguro del ciberespacio y la posibilidad de actuar de forma efectiva frente a conductas irregulares *online* capaces de lesionar los derechos y libertades de las personas o el interés general.

A ello responden, entre otras iniciativas de la Unión Europea, la propuesta de Reglamento sobre Inteligencia Artificial de abril de 2022, actualmente en estudio, o la publicación en el DOUE, el 27 de diciembre pasado, de la Directiva (UE) 2022/2555 –conocida como NIS 2– que sustituirá a la actualmente vigente con la que se pretende establecer medidas de seguridad más estrictas tanto para entidades del sector público como del privado que refuercen su capacidad de resiliencia y de respuesta ante las nuevas amenazas y el riesgo cada vez mayor de ser objeto de ciberataques. Esta Directiva, a su vez, se complementa con otras dos disposiciones de similar finalidad: el Reglamento sobre Resiliencia Operativa Digital en el Sector Financiero (Reglamento DORA), y la Directiva (UE) 2022/2557 (Directiva DREC) sobre resiliencia de entidades críticas, publicadas en el DOUE conjuntamente con la citada Directiva NIS 2.

Más directamente relacionados con la lucha contra la ciberdelincuencia en el marco comunitario, es también de obligada la referencia al futuro Reglamento *e-evidence* sobre conservación y entrega, con fines de investigación criminal, de datos informáticos almacenados en otros países miembros, cuya publicación está prevista para el presente año 2023. También es necesaria la mención a los trabajos en curso para la elaboración del Reglamento *e-Privacy*, sobre respeto de la privacidad y la protección de datos en el sector de las comunicaciones electrónicas, cuyo objetivo es sustituir a la vigente Directiva 2002/58/CE, adaptando su contenido a las necesidades que plantea actualmente la protección de esos bienes jurídicos frente a posibles intromisiones de terceros en contactos interpersonales.

Igualmente, por su incidencia en la investigación de los delitos sexuales que afectan a menores de edad, debe de aludirse al Reglamento que se está elaborando para prevenir y combatir dichas agresiones tanto en el entorno físico como virtual, cuyo origen deriva de la Estrategia de la Unión Europea *para una lucha más eficaz contra el abuso sexual de menores* –COM (2020)607– publicada el 24 de julio de 2020 a la vista de los graves efectos generados en ese ámbito como consecuencia de las medidas de confinamiento adoptadas durante la

pandemia. Tampoco puede omitirse la Propuesta de Directiva sobre lucha contra la violencia de género y violencia doméstica, presentada por la Comisión Europea el día 8 de marzo de 2022 en la que no solo se definen como infracciones penales algunas de las manifestaciones más frecuentes de la violencia de genero digital sino que también se articulan herramientas para la protección de las víctimas de estas conductas, como es el caso de las medidas para hacer inaccesibles en la red los contenidos ilícitos de esta naturaleza.

En relación con este último aspecto ha de destacarse el Reglamento de Servicios Digitales (UE) 2022/2065 de 19 de octubre, publicado en el DOUE el 27 de octubre del pasado año, en el que se definen con precisión las responsabilidades y obligaciones que corresponden a los prestadores de servicios digitales y esencialmente a las plataformas *online* en orden a facilitar la eliminación de estos y otros contenidos ilícitos y de asegurar la protección de los datos personales y los derechos y libertades fundamentales de los ciudadanos y ciudadanas. A dicho fin se establecen mecanismos para garantizar una ágil cooperación entre dichas plataformas y las autoridades nacionales judiciales y administrativas con competencia en esta materia.

Con un ámbito de aplicación territorialmente más amplio, la apertura a la firma del Segundo Protocolo Adicional a la Convención sobre Ciberdelincuencia del Consejo de Europa, en mayo del pasado año 2022, constituye un hito especialmente relevante para impulsar la cooperación internacional contra el cibercrimen. El documento *relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas* ha sido firmado hasta el momento por 35 países, entre ellos España, y su pretensión es la de agilizar los trámites para la obtención transnacional de evidencias electrónicas en condiciones tales de integridad, autenticidad y seguridad que puedan ser utilizadas como medio de investigación o de prueba en un proceso penal.

En la misma línea, pero con proyección universal, son de obligada cita los trabajos en curso para la elaboración de lo que, por el momento, se denomina *Convención Internacional Integral sobre la Lucha contra la Utilización de las tecnologías de la Información y las Comunicaciones con Fines Delictivos.* Se trata de un ambicioso proyecto de NNUU en el que se encuentran implicados la mayoría de los países del mundo y cuyo objetivo es el de aproximar las legislaciones internas de los Estados en aspectos tales como la definición de tipos penales –ciberdependientes y/o ciberhabilitantes–, la articulación de herramientas de investigación criminal y el establecimiento de medidas que faciliten la cooperación transnacional frente a las actividades ilícitas que se planifican y ejecutan en el ciberespacio.

En nuestro país, también se han producido novedades legislativas importantes en esta materia durante el año 2022. Las más significativas son las relativas a determinados tipos penales aplicables a la persecución de ilícitos que se cometen en el ciberespacio. Tal es el caso de la implementación en el Código Penal de la Directiva (UE) 2019/713 sobre fraude y falsificación de medios de pago distintos del efectivo que se ha llevado a efecto por la LO 14/2022, de 22 de diciembre y que ha dado lugar a modificaciones importantes en las figuras delictivas que sancionan las estafas y/o defraudaciones –Capítulo VI del Título XIII del Libro II– y también en los delitos de falsificación de tarjetas de crédito, débito y cheques de viaje –Sección 4.ª del Capítulo II del Título XVIII del Libro II– para adaptarlos a las infracciones penales definidas en la citada Directiva a fin de afrontar con mayor efectividad las nuevas formas de defraudación o falsificación que han ido surgiendo al hilo desarrollo tecnológico.

Igualmente, la publicación de la LO 10/2022 de 6 de septiembre, de *garantía integral de la libertad sexual* ha contribuido a mejorar las herramientas legales para aminorar los graves y perversos efectos de la ciberdelincuencia. Concretamente su disposición final primera incorpora un segundo apartado en el art. 13 de la Ley de Enjuiciamiento Criminal conforme al cual la autoridad judicial, en el curso de la investigación de un delito cometido a través de Internet o de cualquier tecnología de la información y la comunicación, podrá acordar cautelarmente las medidas necesarias para evitar que los contenidos cuestionados permanezcan accesibles a terceros en la red. El reconocimiento procesal de esta posibilidad, que venía demandando este área de especialización en Criminalidad Informática desde hace años, tiene un efecto extraordinariamente positivo para la protección de los intereses de las víctimas de muchos de los ciberdelitos pues, aun cuando dichas medidas hubieran podido acordarse al amparo de los art. 8 y ss. de la ley 34/2002, de 11 de julio, *de Servicios de la Sociedad de la Información y del Comercio Electrónico*, su previsión expresa en la LECrim contribuirá a facilitar su efectiva adopción.

Por su parte, la disposición final cuarta de esa misma LO 10/2022, introduce también novedades significativas en algunos de los tipos penales que sancionan conductas habituales en el entorno virtual, entre ellas, la incorporación de un párrafo quinto en el art. 172 ter CP que define expresamente como delito la utilización no autorizada de la imagen de otra persona para realizar anuncios o abrir perfiles falsos en redes sociales o páginas de contacto causando de este modo a la víctima una situación de humillación o acoso; las modificaciones introducidas en determinados delitos contra la libertad sexual que

ocasionalmente se cometen a través de redes y sistemas informáticos y la tipificación en el párrafo 2.º del art. 197-7 CP de la conducta de quien, sin haber participado en la obtención de imágenes o contenidos audiovisuales de carácter íntimo de otra persona, las difunde o cede sin consentimiento del afectado.

Mas allá de los avances legislativos para la articulación de nuevas y más eficientes herramientas legales contra la ciberdelincuencia, en el año 2022 se han venido impulsando otras iniciativas, ya en curso en años precedentes, con las que se pretende mejorar nuestra capacidad de respuesta frente al uso irregular del ciberespacio. De ello son buen ejemplo, la reestructuración y ampliación de funciones de la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior (OCC) o los distintos grupos de trabajo creados en el marco del Foro Nacional de Ciberseguridad que abordan dicha problemática desde diversos aspectos complementarios entre sí, tales como la adecuación del marco regulatorio o el fortalecimiento de la resiliencia en empresas e instituciones o el fomento de la cooperación público-privada. En estos grupos participan profesionales de distintas áreas –académicos, técnicos, juristas, investigadores– con la finalidad de aunar esfuerzos y compartir experiencias, conocimientos y habilidades en orden a establecer las bases necesarias para cohonestar el aprovechamiento de las ventajas y utilidades que ofrecen las TIC con el reforzamiento de las libertades de los ciudadanos y la protección de sus derechos e intereses y de los principios que sustentan el funcionamiento del Estado de Derecho.