8. CRIMINALIDAD INFORMÁTICA

8.1 **Introducción**

En el momento de iniciar la elaboración de esta Memoria los habitantes de una buena parte de los países del mundo están percibiendo la progresiva vuelta a la normalidad después de muchos meses sometidos inevitablemente a medidas de aislamiento social e incluso de confinamiento más o menos intenso para evitar los riesgos y paliar los efectos de la pandemia causada por el COVID-19. Dicha circunstancia, que determinó que se recurriera a las tecnologías, como medio imprescindible para mantener con la mayor normalidad posible la vida personal y las relaciones con los demás, ha marcado para siempre el planteamiento mismo de la actividad social, económica y política de la humanidad y la propia forma de entender las relaciones personales e institucionales en todos los ámbitos de la actividad humana, ya indefectiblemente vinculada al uso de las herramientas TIC. Esta nueva situación, cuyas ventajas son claramente perceptibles, entraña también importantes riesgos derivados de esa mayor exposición a las ciberamenazas, si, como ocurre frecuentemente, esa intensa penetración de las tecnologías en el entramado social no va acompañada de las medidas de seguridad adecuadas para garantizar, también en el ciberespacio, los intereses individuales y colectivos y los derechos y libertades públicas de todas las personas.

Conscientes de esa profunda digitalización social y de la indiscutible incidencia de las tecnologías en el progreso y desarrollo de la humanidad, en el año 2021 se ha hecho evidente el esfuerzo empeñado por los poderes públicos de todos los Estados del mundo, y en particular los de nuestro entorno más próximo, para promover e impulsar líneas de acción que mejoren la protección frente a los riesgos derivados de un uso irregular del ciberespacio. Se trata de cohonestar el aprovechamiento efectivo de las extraordinarias posibilidades de acción que ofrecen las TIC con el reforzamiento de la ciberseguridad en todos los ámbitos.

Este es el planteamiento que subyace en el documento *Nest Generation EU,* publicado en mayo del año 2021, en el que, al hilo de los trabajos de elaboración de una nueva Estrategia de Ciberseguridad, la Comisión Europea reflexiona acerca de cómo la pandemia ha evidenciado *la importancia de la digitalización en todas las áreas de la economía,* derivando de ello, a medio o largo plazo, *cambios permanentes y estructurales en la vida social y económica,* entre los que menciona la popularización del teletrabajo y la progresiva implantación de la

formación en línea, el comercio electrónico y la Administración digital. En igual sentido, la Resolución del Parlamento Europeo de 10 de junio de 2021, dedicada a ese mismo tema, recuerda que, si bien la *transformación digital es una prioridad estratégica clave de la Unión,* dicha transición se encuentra *asociada a una mayor exposición a las ciberamenazas* tales como los ciberataques contra infraestructuras críticas, las amenazas híbridas o las campañas de desinformación y exhorta a los Estados y a las Instituciones de la Unión a promover *el desarrollo de redes y sistemas de información, infraestructuras y conectividad seguros y fiables en* todo el territorio comunitario, al tiempo que *subraya que la ciberseguridad debe estar integrada en la digitalización* de los diversos sectores sin olvidar que todos ellos están interconectados y que *las deficiencias en un sector pueden causar dificultades en otro.* En consecuencia, el Parlamento Europeo apuesta por políticas de ciberseguridad en la Unión que sean *coherentes e interoperables en todos los sectores.*

Sería imposible resumir en estas breves líneas las diversas actuaciones que integran el ambicioso proceso legislativo actualmente en curso en el marco comunitario para materializar el planteamiento antes expuesto. Entre las más significativas, y que más directamente se relacionan con la actividad que nos ocupa, hay que citar el Reglamento sobre Servicios Digitales *–Digital Service Act (DSA)–* cuya propuesta ha sido aprobada por el Parlamento Europeo el 20 de enero de este mismo año- con el que se pretende definir con mayor precisión las responsabilidades y obligaciones de los prestadores de servicios digitales y esencialmente de las plataformas en línea, de forma tal que se asegure la protección de los datos personales y de los derechos y libertades fundamentales de los ciudadanos y ciudadanas y se facilite la eliminación en la red de contenidos ilícitos, potenciando y mejorando a dicho fin la cooperación entre dichas plataformas y las autoridades nacionales, judiciales y administrativas, con competencia en esas materias. También es de obligada cita el Reglamento *e-Privacy*, *sobre respeto de la vida privada y protección de datos en el sector de las comunicaciones electrónicas,* que sustituirá a la vigente Directiva 2002/58/CE, relativa al mismo tema, adaptando su contenido a los riesgos que generan los actuales canales de comunicación con el objetivo de proteger de forma más estricta la privacidad frente a posibles intromisiones de terceros en los contactos interpersonales.

Otros proyectos en marcha de especial interés son el Reglamento sobre Mercados Digitales *–Digital Markets Act (DMA)–* que pretende regular las prácticas comerciales de las grandes plataformas *online* y su capacidad de control sobre los datos personales de los/las habitan-

tes en Europa y clarificar las atribuciones de las autoridades nacionales de competencia en esta materia; la Directiva NIS 2, que da un paso adelante en la regulación desarrollada por la conocida como Directiva NIS –*Network and Information Security*– (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio, *sobre seguridad de las redes y sistemas de información*- ampliando el espectro de entidades y organismos sometidos a las obligaciones establecidas en materia de seguridad lógica y notificación de incidentes y apostando por una mayor armonización normativa en temas de prevención, respuesta y detección de las ciberamenazas y ciberataques; o las iniciativas en curso para articular un marco regulatorio común sobre criptomonedas, cuyo más significativo exponente es el Reglamento MICA –*Markets in Crypto Asses*–.

La lucha contra la ciberdelincuencia constituye un aspecto esencial en esta apuesta por la seguridad en el ciberespacio, por lo que el impulso legislativo para dar uniformidad a la normativa de los Estados, tanto en lo relativo a la tipificación de nuevas conductas como a la articulación de medidas de protección, de investigación tecnológica y de cooperación internacional, está siendo particularmente intenso. Al respecto, pueden citarse a modo de ejemplo el Reglamento (UE) 2021/784 del Parlamento Europeo y del Consejo, de 29 de abril *sobre la lucha contra la difusión de contenidos terroristas en línea,* recientemente publicado, o los trabajos en curso sobre el Reglamento *e-evidence*, *sobre conservación y entrega de datos informáticos almacenados en otro país miembro de la Unión*, a efectos de facilitar la obtención transnacional de evidencias electrónicas con fines de investigación criminal; y también los relativos a la elaboración de una Estrategia Europea contra el abuso sexual infantil tanto en el entorno físico como virtual, sin olvidar tampoco la Resolución del Parlamento Europeo de septiembre de 2021 que apuesta por considerar la violencia de género, incluida la de carácter digital, como actividad delictiva merecedora de tratamiento unificado en la UE, al amparo del art. 83.1del TFUE.

Por su parte, y en el marco de la cooperación internacional contra la delincuencia en el ciberespacio, constituye un hito esencial la aprobación del Segundo Protocolo Adicional a la Convención de Budapest sobre Ciberdelincuencia del CoE, en el que se regulan nuevos mecanismos jurídicos para la obtención transnacional de evidencias electrónicas con fines de investigación criminal, cuya utilización va a potenciar extraordinariamente la colaboración en esta materia entre los 66 países del mundo que, hasta el momento, han suscrito el indicado tratado internacional.

Este mismo proceso de toma de conciencia e impulso de medidas estratégicas, legales u organizativas para hacer posible la seguridad en el ciberespacio se viene produciendo desde hace varios años en España. De ello da cuenta la publicación en abril de 2019 de la vigente Estrategia Nacional de Ciberseguridad que, sustituyendo a la aprobada en 2013, fijó la posición del Estado ante la nueva concepción de la ciberseguridad en el marco de la Política de Seguridad Nacional. También en este ámbito interno son muchas las iniciativas adoptadas desde entonces, siguiendo la estela marcada por dicha Estrategia y también por la evolución de la normativa comunitaria y la propia percepción de las necesidades que se han ido generando en esta materia. Entre ellas han de citarse, el Real Decreto 43/2021 de 26 de enero, que culmina el desarrollo legislativo interno para la completa implementación de la Directiva NIS (UE) 2016/1148, antes citada, o la publicación del Real Decreto 1150/2021, de 28 de diciembre, que aprueba una nueva Estrategia de Seguridad Nacional uno de cuyos vectores es precisamente la transformación digital y la necesidad de proteger la seguridad en el ciberespacio.

En este marco, la actuación frente a la ciberdelincuencia se plantea en nuestro país como medio de garantizar la seguridad ciudadana y de salvaguardar los derechos y libertades de los/las ciudadanos/as en el entorno digital. A esos efectos, la Estrategia Nacional de Ciberseguridad de 2019 define la cibercriminalidad como el conjunto de actividades ilícitas cometidas en el ciberespacio contra elementos o sistemas informáticos o contra cualesquiera otros bienes jurídicos siempre que en su planificación, desarrollo o ejecución resulte determinante el uso de herramientas tecnológicas, definición muy similar a la recogida en la Instrucción 2/2011 *sobre el Fiscal de Sala de Criminalidad Informática y las secciones de Criminalidad Informática de las Fiscalías.*

También en esta materia se han producido novedades significativas en el año memorial, entre las que destacamos, por su importancia, la publicación de la Ley Orgánica 7/2021 de 26 de mayo de *protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales,* que incorpora al ordenamiento jurídico español la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril, así como la de la Ley Orgánica 8/2021 de 4 de junio *de protección integral de la infancia y adolescencia frente a la violencia* que, en su disposición final sexta, introduce modificaciones importantes en el Código Penal, entre ellas, la tipificación de determinadas conductas online que atentan contra bienes jurídicos de las personas menores de edad e, igualmente, la tramitación del proyecto de ley para

la implementación de la Directiva (UE) 2019/713 *sobre falsificación de medios de pago distintos del efectivo*, cuya próxima aprobación, en el presente año, afectará a muchos de los tipos penales actualmente vigentes sobre falsedad y estafa.

Aunque su incidencia en la lucha contra la ciberdelincuencia es más indirecta, no podemos dejar de mencionar el Real Decreto Ley 7/2021 de 27 de abril que, entre otras, transpone al ordenamiento jurídico español la Directiva (UE) 2018//843 del Parlamento y del Consejo, de 30 de mayo, y modifica la Ley 10/2010 de 28 de abril *sobre prevención de la utilización del sistema financiero para el blanqueo de capitales y la financiación del terrorismo,* en el sentido de considerar sujetos obligados a esos efectos a los proveedores de servicios de intercambio de moneda electrónica por moneda de curso legal y a los de custodia de monederos virtuales.

Finalmente, en 2021 también se han producido, en esta materia, otras novedades importantes en el marco de la propia Institución, entre ellas, la publicación en el mes de marzo del *Protocolo para combatir el Discurso de Odio Ilegal en línea,* al que nos referiremos más adelante con mayor detalle; la actualización en septiembre de 2021 de la Instrucción 2/2011 *sobre el Fiscal de Sala de Criminalidad Informática y las secciones de Criminalidad Informática de las Fiscalías* y la participación activa del Ministerio Fiscal en la elaboración del Plan Estratégico contra la Cibercriminalidad, impulsado por la Secretaría de Estado del Ministerio del Interior y en la que también intervinieron, entre otras instituciones, el Consejo General del Poder Judicial, el Consejo General de la Abogacía y diversos organismos policiales (CITCO [1], CNPIC [2], OCC, etc.).

[1] Centro de Inteligencia contra el Terrorismo y el Crimen Organizado.
[2] Centro Nacional de Protección de Infraestructuras Críticas y Ciberseguridad.