8. CRIMINALIDAD INFORMÁTICA

8.1 **Introducción**

La evolución tecnológica sigue avanzando inexorablemente y dejando su impronta en todos los ámbitos de la actividad humana. La utilización cada vez más frecuente de los recursos de la inteligencia artificial en determinados ámbitos de la vida cotidiana o de las relaciones sociales, el creciente aprovechamiento de las tecnologías *blockchain* para el registro y gestión de procesos complejos –no solo en el sector privado sino también en determinadas actuaciones de entidades públicas–, o la definitiva implantación de la red móvil de quinta generación (5G), con sus extraordinarias consecuencias en la velocidad de las comunicaciones o en el Internet de las cosas, son solo algunos ejemplos de la trascendencia de dicho proceso evolutivo y de la profundidad con la que los imparables avances en la ciencia y la tecnología van alcanzando y capilarizando todas las facetas de la vida de las personas y de las relaciones sociales, políticas o económicas.

En el momento de redactar estas líneas, todos los ciudadanos españoles, al igual que los de una buena parte de los países del mundo, nos hemos visto obligados a un estricto régimen de confinamiento como consecuencia de la pandemia por la enfermedad COVID 19, que nos ha llevado a la utilización de las Tecnologías de la Información y la Comunicación (en adelante TIC) como medio casi imprescindible para mantener cualquier clase de relación con las personas, a excepción de aquellas con las que compartimos la situación de aislamiento. Dicha circunstancia extraordinaria, entre otras muchas y profundas consecuencias, nos ha servido de experiencia para constatar hasta qué punto es posible canalizar nuestra actividad profesional y nuestros contactos con los demás a través de estas herramientas tecnológicas, así como para percibir las grandes ventajas y facilidades que nos aportan, pero también da fe de los riesgos que entraña su utilización si no se observa la debida prudencia y se prescinde de las medidas de seguridad adecuadas. Tiempo habrá de reflexionar sobre esta experiencia cuando contemos con la información necesaria para efectuar las oportunas valoraciones, si bien, por el momento, se puede a afirmar que el uso intensivo de las TIC al que se han visto abocados los ciudadanos y las habilidades adquiridas al respecto traerán consigo una más profunda e intensa penetración de estas tecnologías en el planteamiento y organización de la actividad social y en el desenvolvimiento de la vida de las personas.

Todo ello está repercutiendo igualmente en el ámbito de la delincuencia. Ese aumento drástico del uso de las tecnologías ha incremen-

tado también el riesgo de que se produzcan en el propio entorno virtual ataques contra los diversos bienes jurídicos objeto de protección penal. En estos días, mayo de 2020, se constata claramente como los delincuentes han sabido aprovechar las vulnerabilidades derivadas de las actuales circunstancias y acomodar a dicho fin la planificación y ejecución de sus criminales acciones. Sin profundizar en ello, es posible dejar constancia de algunos de sus efectos: un repunte muy importante en las actividades relacionadas con la distribución *online* de material pornográfico –constatado en base a indicadores nacionales e internacionales–, la focalización de las actividades fraudulentas en la oferta de productos médico-farmacéuticos o de servicios relacionados con la protección personal contra el patógeno (mascarillas, EPIs, etc.) o de bienes y/o prestaciones útiles para aliviar la situación de confinamiento (servicios de entretenimiento *online,* aparatos de mantenimiento físico, equipos electrónicos, etc.) y también la captación de datos personales, ya sea mediante engaño (simulando actuar en nombre de empresas de energía, entidades bancarias, etc.) o mediante el acceso irregular a sistemas informáticos para su utilización posterior con finalidades fraudulentas. Cuál haya sido la efectiva incidencia de esta situación excepcional en la ciberdelincuencia y cómo repercutirá en la evolución del fenómeno criminal que nos ocupa es algo que iremos analizando en un futuro próximo.

Con todo, la necesidad de proteger a los ciudadanos del uso irregular de las tecnologías, en particular frente a las actividades delictivas que se planifican y ejecutan en el ciberespacio, ha determinado en el año 2019 avances significativos en el marco regulatorio nacional. Concretamente ha de reseñarse la publicación el 30 de abril de la actual Estrategia Nacional de Ciberseguridad, que sustituye a la publicada en 2013 y fija la posición del Estado ante la nueva concepción de la ciberseguridad en el marco de la Política de Seguridad Nacional. Uno de los objetivos de esta Estrategia es el de hacer posible un uso seguro del ciberespacio, a cuyo desarrollo se orienta la línea de acción tercera con la que se pretende reforzar las capacidades de investigación y persecución de la cibercriminalidad como medio de garantizar la seguridad ciudadana y la protección de derechos y libertades de los ciudadanos en el entorno virtual. A esos efectos, 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 la utilización de herramientas tecnológicas, definición muy próxima a la que realizó la Fiscalía General del Estado en la *Instrucción 2/2011 sobre el Fiscal de*

Sala de Criminalidad Informática y las Secciones de Criminalidad Informática de las Fiscalías.

También en el año 2019 se ha llevado a efecto la tramitación del Anteproyecto de Ley Orgánica para la Protección Integral de la Infancia y la Adolescencia frente a la Violencia que, entre otras novedades y en lo que aquí interesa, apuesta por la incorporación de nuevos delitos en el texto penal sustantivo que permitan actuar penalmente frente a determinadas conductas *online* contra menores de edad, como la incitación al suicidio, a la autolesión, o al consumo/uso de productos o tratamientos que pueden provocar trastornos alimentarios. Igualmente, dicho anteproyecto hace suya la pretensión de la Fiscalía de contemplar, en un nuevo apartado del art. 13 LECrim, la posibilidad de que el órgano judicial acuerde con carácter cautelar, en cualquier clase de delitos, la adopción de las medidas necesarias para la eliminación o bloqueo de acceso a contenidos ilícitos cuya permanencia en la red resulte perjudicial para el interés general o el de la propia víctima de la acción ilícita.

En el marco de la Unión Europea, durante el pasado año se realizaron también importantes esfuerzos en la lucha contra la delincuencia en la red. Buen ejemplo de ello es la publicación de la *Directiva (UE) 2019/713 de 17 de abril sobre fraude y falsificación de medios de pago distintos del efectivo*, pendiente de incorporación al ordenamiento jurídico español, uno de cuyos ejes de acción es la lucha contra el fraude cometido a través de los sistemas informáticos, así como los trabajos en curso para la elaboración de dos grandes proyectos normativos: de un lado el Reglamento sobre Privacidad y Comunicaciones Electrónicas, más conocido como Reglamento *e-privacy*, con el que se pretende actualizar la vigente Directiva 2002/58/CE, relativa al tratamiento de los datos personales y protección de la intimidad en el sector de las comunicaciones, y reforzar, en último término, la privacidad de los usuarios; y de otro, el Reglamento *e-evidence,* cuyo objetivo es articular una orden europea para la conservación y entrega de datos informáticos almacenados en cualquiera de los países miembros de la Unión, a efectos de facilitar la obtención transnacional de evidencias electrónicas en ese espacio común.

A su vez, en el Consejo de Europa se sigue avanzando en la elaboración de un Segundo Protocolo Adicional a la Convención de Budapest sobre Ciberdelincuencia dedicado específicamente a mejorar los instrumentos para facilitar y agilizar la obtención transnacional de evidencias almacenadas en sistemas informáticos.