# 8. CRIMINALIDAD INFORMÁTICA

## 8.1 **Introducción**

Un año más se inicia esta Memoria con una reflexión acerca de la rapidez e intensidad con que evolucionan las tecnologías de la información y comunicación y de la incidencia que esa evolución tiene en todas las facetas de la convivencia humana; en las relaciones sociales, políticas y económicas; en la actividad de los organismos e instituciones nacionales e internacionales, públicos y privados y en las relaciones entre los Estados.

Un gran parte del conjunto de actuaciones en las que se articula la estructura y el funcionamiento de la sociedad actual se desarrollan en el ciberespacio, concepto que hace referencia a un entorno de carácter no físico creado por equipos de cómputo unidos para interoperar en una red o, como lo define nuestro diccionario de la RAE, un ámbito virtual creado por medios informáticos. En cualquier caso, como recuerda en su Preámbulo la Directiva 2013/40/UE del Parlamento europeo y del Consejo, es un hecho incuestionable que *los sistemas de información son un elemento esencial para la interacción política, social y económica,* hasta el punto de que *la dependencia de este tipo de sistemas por parte de la sociedad es muy grande y sigue aumentando,* razón por la cual, en consecuencia, garantizar el uso seguro del ciberespacio a partir de la protección de la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, preservando al tiempo el pleno ejercicio de los derechos y las libertades de las personas, constituye hoy por hoy uno de los grandes desafíos a los que se enfrenta la comunidad internacional.

Este objetivo impulsa desde hace años los trabajos que se desarrollan en los distintos foros internacionales y también en nuestro país, tratando de obtener la adecuación de las normas legales a esta nueva realidad que afecta a los distintos aspectos en los que se desenvuelve la actividad humana. Buen ejemplo de ello es, sin duda, el esfuerzo empeñado en el marco de la Unión Europea para reforzar en todos los ámbitos la protección de los datos personales frente a los riesgos y amenazas derivadas de la creciente capacidad de tratamiento y almacenamiento de información de las herramientas tecnológicas, siguiendo, a esos efectos, las pautas fijadas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. La publicación de dicho Reglamento, cuya incidencia en la actividad ordinaria de toda persona física o jurídica, organismo o institución que por su actividad gestione datos personales es claramente perceptible, se ha concretado

en España en la publicación de la LO 3/2018 de 5 de diciembre de Protección de Datos Personales y Garantía de los Derechos Digitales.

A similar planteamiento obedece el proyecto de Reglamento sobre Privacidad y Comunicaciones Electrónicas, más conocido como Reglamento *e-privacy*, que se encuentra en fase de elaboración en el marco de la UE con la pretensión de actualizar la vigente Directiva 2002/58/CE, sobre tratamiento de los datos personales y protección de la intimidad en el sector de las comunicaciones, y de reforzar, en último término, la privacidad de los usuarios.

Por su parte y en lo que se refiere más concretamente a la ciberseguridad, el año 2018 trajo consigo la publicación del Real Decreto-ley 12/2018, de 7 de septiembre, por el que se incorpora al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, también conocida como Directiva NIS, documento clave en el planteamiento preventivo europeo frente al uso irregular del ciberespacio a partir de la identificación de los sectores y operadores críticos y del establecimiento de exigencias de notificación de incidentes de ciberseguridad.

En nuestro país, en 2018, la preocupación por la seguridad en el ciberespacio se ha concretado en la puesta en marcha por acuerdo del Consejo de Seguridad Nacional publicado por Orden PCI/870/2018 de 3 de agosto, del proceso para la elaboración de una nueva Estrategia de Ciberseguridad Nacional que sustituya a la publicada en diciembre de 2013, con la finalidad de ofrecer una mejor respuesta a las amenazas de seguridad emergentes en redes y sistemas de información y, en definitiva, adaptarla a las dinámicas de transformación de la seguridad global. Dicho esfuerzo ha culminado con la publicación en el BOE de 30 de abril de 2019 de la actual Estrategia de Ciberseguridad Nacional, documento que, al igual que la de 2013, aborda entre sus directrices la lucha frente a la delincuencia en la red, en el entendimiento de que la utilización de las TIC con fines delictivos no es sino uno de los efectos del uso irregular del ciberespacio.

Pues bien, centrándonos en este último aspecto, cuyo análisis es el objetivo de esta Memoria, es incuestionable el efecto que el desarrollo tecnológico está teniendo en la mayoría de las actividades delictivas, dando lugar a un cambio progresivo en su planificación y ejecución para aprovechar las ventajas y potencialidades que ofrecen las herramientas informáticas. Esta realidad determinó que el legislador español, inicialmente por LO 5/2010 y posteriormente por las también Leyes Orgánicas 1/2015 y 2/2015, abordara una importante reforma del Código Penal, a día de hoy plenamente consolidada en la práctica habitual de nuestros Tribunales que supuso la incorporación a nuestro

texto penal sustantivo de nuevas figuras delictivas y la redefinición de las ya existentes para poder actuar frente a las nuevas formas de lesión. Pese al profundo calado de dicha reforma, es un hecho cierto que continuamente detectamos otras necesidades de tipificación penal a medida que el progreso tecnológico ofrece posibilidades no previstas de atentar contra bienes jurídicos precisados de protección. Por ello, no sorprende que el Anteproyecto de Ley Orgánica para la Protección Integral de la Infancia y la Adolescencia frente a la Violencia haya contemplado la incorporación de nuevos delitos para sancionar conductas que se están ejecutando a través de Internet contra menores de edad, como la incitación al suicidio y la autolesión, al consumo de productos o la utilización de tratamientos que pueden provocar trastornos alimentarios. Como tampoco sorprenderá que, al igual que en años anteriores, insistamos en esta memoria en la oportunidad de tipificar como delito autónomo la suplantación de identidad en la red.

La necesidad de evitar que la difusión de contenidos a través de la red prolongue indefinidamente las consecuencias del delito y sus perversos efectos tanto para las víctimas como para el interés general ha determinado que se dé una especial atención a la posibilidad de hacer inaccesibles dichos contenidos. A ello se refiere expresamente la Recomendación (UE) 2018/334 de 1 de marzo de la Comisión sobre medidas para combatir eficazmente los contenidos ilícitos en línea, al igual que la Directiva (UE) 2017/541 del Parlamento y del Consejo sobre lucha contra el terrorismo que, en su artículo 21, insta a los Estados a la adopción de las medidas precisas para la rápida eliminación de contenidos de esa naturaleza o para bloquear el acceso a los mismos. También en España el Anteproyecto de Ley Orgánica de Protección de la Infancia antes mencionado, con igual objetivo, propone la inclusión de un segundo apartado en el art 13 de la Ley de Enjuiciamiento Criminal, en el que, como medida cautelar, se generalice esa posibilidad en el curso de la tramitación de procesos penales por cualquier tipo de delito cometido a través de la red.

Pero, con todo, las mayores dificultades ante este fenómeno criminal se plantean en el ámbito de la investigación criminal. Es evidente que las capacidades que ofrecen las herramientas tecnológicas pueden y deben ser utilizadas para el esclarecimiento de los hechos delictivos y la determinación de sus autores, pero ello ha de hacerse con las garantías y salvaguardas exigibles en el proceso penal y con pleno respeto a los derechos y libertades de los ciudadanos y, en particular, de las personas investigadas. El legislador español imprimió un gran impulso en este ámbito con la incorporación a la legislación interna, por LO 13/2015 de 5 de octubre, de una regulación completa y deta-

llada de la utilización de mecanismos y herramientas propios de la investigación tecnológica. Pero también en esta materia continuamente van surgiendo controversias técnicas y jurídicas en el esfuerzo cotidiano por cohonestar la eficacia en la investigación con el cumplimiento estricto de las garantías y exigencias del Estado de Derecho, cuya complejidad se ve incrementada a causa de la dimensión transnacional de éste fenómeno criminal que hace imprescindible la coordinación entre autoridades de unos y otros Estados.

Así, en el último año, en el marco de la Unión Europea se ha trabajado intensamente en la elaboración de un Reglamento con el que, a partir del principio de reconocimiento mutuo, se pretende articular la futura Orden Europea para la conservación y obtención de datos informáticos almacenados por operadores o proveedores ubicados fuera del territorio del Estado requirente. Al tiempo que, en otro ámbito que también nos es muy próximo, el del Consejo de Europa y con participación activa de esta Fiscalía, se está trabajando en la elaboración de un Segundo Protocolo Adicional a la Convención de Budapest sobre Ciberdelincuencia con el doble objetivo de impulsar la armonización normativa sobre utilización de herramientas de investigación tecnológica y reforzar la cooperación internacional en relación con ello.

El gran debate que se está generando tanto a nivel nacional como internacional respecto a la delimitación de los parámetros a que debe ajustarse cualquier investigación que verse sobre datos y sistemas informáticos, o que se sirva de las TIC con esa finalidad, está también determinando importantes pronunciamientos de nuestros Tribunales y de los Tribunales internacionales. Ante la imposibilidad de analizarlos de forma exhaustiva nos limitamos a citar el que más directamente afecta al Estado español, la Sentencia del TJUE de 2 de octubre pasado, en el que se resuelve una cuestión prejudicial planteada por la Audiencia Provincial de Tarragona en el sentido de considerar que *aplicando criterios de proporcionalidad, una injerencia grave en derechos fundamentales, con ocasión de la prevención, investigación y persecución de delitos, solo podría estar justificada cuando el objetivo sea el de actuar contra un delito grave. Sin embargo, si la injerencia no es de carácter grave podría estar justificada, aun cuando el delito que se investiga o persigue no tenga la consideración de grave.*