8. CRIMINALIDAD INFORMÁTICA

8.1 **Introducción**

A mediados de mayo del pasado año 2017 la comunidad internacional observó con asombro como, en unas pocas horas, un virus informático conocido como *WannaCry* puso en alerta todos los mecanismos de seguridad y de protección de los sistemas informáticos de medio mundo al generar una infección que afectó directa o indirectamente a unos 300.000 equipos, en más de 150 países de distintos ámbitos geográficos, con la que se pretendía cifrar la información e imposibilitar el acceso por parte de sus titulares a los datos alojados en los sistemas atacados. Transcurrido poco más de un mes, otro ataque cibernético, esta vez provocado por el virus *NotPetya*, provocó riesgos similares en entidades del sector público y empresas dedicadas a la energía y las telecomunicaciones. Ciertamente, los efectos reales de ambos ataques fueron de escasa entidad, pero sirvieron para poner de manifiesto su potencialidad y capacidad de difusión, el riesgo efectivo que entrañan y las graves consecuencias que pueden tener en el normal funcionamiento de organismos e instituciones de todo tipo e incluso en el desenvolvimiento de las relaciones políticas, sociales y/o económicas nacionales e internacionales. Este riesgo potencial ya había sido reflejado por el legislador comunitario en el Preámbulo de la Directiva 2013/40/UE del Parlamento europeo y del Consejo en el que se recuerda que «los sistemas de información son un elemento esencial para la interacción política, social y económica y que la dependencia de este tipo de sistemas por parte de la sociedad es muy grande y sigue aumentando, alertando, al tiempo, de la amenaza creciente para la Unión de dichos ataques que ponen en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia y exige, por tanto, una respuesta por parte de la Unión, así como una cooperación y coordinación reforzadas a escala internacional».

Precisamente por ello, lograr establecer unos parámetros que garanticen el uso seguro del ciberespacio es uno de los desafíos a los que se enfrenta la sociedad actual, y uno de los aspectos que centran la atención de los Gobiernos de los diversos países del mundo y de los organismos e instituciones internacionales con responsabilidad en esta materia. Se trata, en definitiva, de aprovechar las ventajas que ofrece el desarrollo tecnológico para una mejor y más completa progresión social, pero garantizando, al tiempo, el pleno respeto a los derechos y libertades fundamentales de las personas y los principios y valores que sustentan nuestro orden jurí-

dico y social y nuestro modelo de convivencia democrática y libre. A ello se refiere expresamente la Estrategia de Ciberseguridad de la Unión Europea (en adelante, UE), publicada en 2013, al indicar que «la ciberseguridad solo puede resultar positiva y eficaz si se basa en los derechos fundamentales y las libertades enunciados en la Carta de Derechos Fundamentales de la UE, al tiempo que recuerda que los derechos individuales no pueden protegerse si no es a través de redes y sistemas seguros». Y así lo ha entendido también, recientemente, la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo en la propuesta de Resolución sobre Lucha contra la Ciberdelincuencia, presentada a aprobación en el mes julio del pasado año 2017, que se hace eco expresamente de esta misma idea.

A partir de este planteamiento son muchas las iniciativas legislativas nacionales e internacionales que se han ido llevando a efecto para garantizar la protección de este sistema de valores frente a los nuevos y crecientes riesgos derivados de las potencialidades y capacidades de las tecnologías de la información y la comunicación (en adelante TIC). Por ceñirnos a algunas de las que han ocupado la agenda legislativa en nuestro país en 2017, y sin pretensión de exhaustividad, son de obligada mención los trabajos en curso para la adaptación de nuestra normativa interna sobre protección de datos al nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, sobre esa misma materia, con el que el legislador comunitario pretende ofrecer un marco de protección más sólido, coherente y eficaz a los datos personales superando las insuficiencias detectadas en la aplicación de la añeja Directiva 95/46/CE como consecuencia de los factores antes indicados. E igualmente el proyecto legislativo en curso para incorporar a nuestro ordenamiento jurídico la Directiva 2016/1148/UE del Parlamento Europeo y del Consejo, *relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión* –conocida como Directiva NIS-centrada especialmente en reforzar la detección y prevención de ataques informáticos.

En este marco, la ciberdelincuencia no es sino uno de los efectos –posiblemente uno de los más graves y peligrosos– de ese uso irregular de las tecnologías y así ha de entenderse, desde nuestro punto de vista, si pretendemos ofrecer soluciones que combinen eficazmente los aspectos preventivos con la respuesta penal desde el Estado de Derecho ante estas conductas. Es un fenómeno criminal que extiende su radio de acción a una pluralidad de manifestaciones delictivas como consecuencia inevitable del uso generalizado de las herramientas tecnológicas en todas las facetas de la actividad humana,

de tal forma que, en la actualidad, son pocas las conductas ilícitas extrañas al uso de estas tecnologías. Obviamente, no es este el momento de profundizar en lo que ha de considerarse por ciberdelincuencia, concepto que circunscribimos, a los efectos que nos ocupan, a los parámetros definidos en la Instrucción 2/2011 de la Fiscalía General del Estado *sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías*, sino más bien de reflexionar acerca de su incidencia en el último periodo anual y de la evolución de sus distintas manifestaciones al hilo de las nuevas posibilidades que ofrece el imparable desarrollo tecnológico.

El legislador internacional y nacional es plenamente consciente de la versatilidad del fenómeno y de su potencialidad para concretarse en nuevas y diferentes formas de atacar bienes jurídicos, merecedores de protección penal, así como de la necesidad de articular herramientas de investigación adecuadas para combatir esta forma de delincuencia. A ello responden, en el ámbito interno, las acertadas reformas operadas, en el año 2015, en el Código Penal y en la Ley de Enjuiciamiento Criminal. Y, en línea con ese esfuerzo normativo, el Ministerio Fiscal ha venido aportando su especial contribución, de la que es un buen ejemplo la publicación de la Circular 3/2017, elaborada en esta Unidad de Criminalidad Informática y en la que se analizan los nuevos tipos penales que sancionan las diversas formas de ataques a los sistemas de información.

Pero estamos en un proceso dinámico e imparable y la detección de nuevas necesidades –algunas de las cuales comentaremos en este trabajo– obliga indefectiblemente a seguir planteando avances legislativos o medidas de carácter operativo u organizativo que refuercen y garanticen la eficacia del Estado ante esta forma de delincuencia.