Aspectos jurídicos de la ciberseguridad

Aspectos jurídicos de la ciberseguridad

Ofelia Tejerina (coordinadora de la obra)
Marta Beltrán (coordinadora de la colección)

Ra-Ma®

La ley prohíbe
fotocopiar este libro

Editado por:
RA-MA Editorial
Calle Jarama, 3A, Polígono Industrial Igarsa
28860 PARACUELLOS DE JARAMA, Madrid
Teléfono: 91 658 42 80
Fax: 91 662 81 39
Correo electrónico: *editorial@ra-ma.com*
Internet: *www.ra-ma.es* y *www.ra-ma.com*
ISBN: 978-84-9964-971-9
Depósito legal: M-16723-2020
Maquetación: Antonio García Tomé
Diseño de portada: Antonio García Tomé
Filmación e impresión: Safekat
Impreso en España en julio de 2020

ÍNDICE

PRÓLOGO

La Ciberseguridad es un campo eminentemente técnico, pero como ya hablamos en el primer libro de esta colección, no lo es exclusivamente. Cada vez más, los equipos que trabajan en esta disciplina incorporan perfiles relacionados con la economía, la ética, las leyes, los recursos humanos. Es por ello por lo que en esta colección nos hemos propuesto no descuidar estos aspectos y dedicarles, poco a poco, libros que sirvan como una primera aproximación para aquellos estudiantes y profesionales de la Ciberseguridad que necesiten asomarse a esas otras disciplinas, menos comunes o conocidas, pero imprescindibles para su labor en la actualidad. En este segundo libro de la colección comenzamos por analizar los aspectos jurídicos de la ciberseguridad. Creemos que los abogados tienen un papel protagonista en la gestión de incidentes de seguridad o de brechas de datos, por mencionar sólo un par de ejemplos. Y los roles tradicionalmente tecnológicos deben conocer el marco regulatorio en el que operan sus organizaciones y las consecuencias de las decisiones que toman, por poner también otro par de ejemplos.

Pasando de la esfera profesional a la personal o particular, hay que recordar que la primera Estrategia Nacional de Ciberseguridad que tuvimos en España data del año 2013, pero que se ha ido actualizando cada año para destacar los principales retos a los que nos enfrentamos como sociedad con el progreso de la tecnología. Se destacaba ya entonces que "los distintos perfiles de atacantes que explotan las vulnerabilidades tecnológicas con el objeto de recabar información, sustraer activos de gran valor y amenazar los servicios básicos, pueden afectar al normal funcionamiento de nuestro país. El disfrute pacífico de ciertos derechos fundamentales consagrados en nuestra Constitución y en el ordenamiento jurídico internacional puede verse seriamente comprometido como consecuencia de este tipo de acciones". Es decir, que su normalización como parte de nuestra vida era evidente, y que ya no estamos solo ante una preocupación de grandes multinacionales o de gobiernos y espías, no

es solo cosa de hackers (expertos en informática) y ciberdelincuentes, ni es ciencia ficción.

La ciberseguridad nos afecta a todos como individuos y en casi todos los aspectos de nuestro desarrollo social. Afecta a nuestros derechos más fundamentales, como la intimidad o la protección de datos, la libertad de expresión e información, pero también a derechos de corte socioeconómico, como la propiedad "digital" o el teletrabajo, y la legislación no puede ser ajena a todo ello, ni nosotros podemos ignorarla (*ignorantia iuris non excusat*).

El marco jurídico ha experimentado una importante evolución en este sentido, desde las normas que reformaron los códigos penal y procesales, o las que regulaban la firma electrónica o el comercio electrónico, a la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, o la última reforma de la Ley de protección de datos que fue aprobada en 2018 para adaptarla al Reglamento Europeo de Protección de Datos (RGPD). El Derecho interno tiene que ordenar cada uno de los aspectos que se derivan de las nuevas formas de convivencia, o más bien, de su uso, que permite esa convivencia digital. Pero el Derecho no puede ir al mismo ritmo, y no debe. El Derecho debe ser consciente de que su tarea conlleva tácitamente un objetivo de permanencia en el tiempo, y que con la tecnología esto no puede lograrse si se busca entrar a considerar de inmediato cada elemento innovador que aparece en nuestra vida. Antes de ayer hablábamos de ordenadores y programas informáticos, ayer hablábamos de móviles y apps, y hoy de ética e inteligencia artificial. Incluso una pandemia, como la del COVID-19, puede obligarnos de forma urgente a reconfigurar nuestros esquemas sobre su buen uso en situaciones excepcionales y a adaptarnos a nuevas opciones tecnológicas que ni siquiera nos habíamos planteado que pudieran normalizarse, como la trazabilidad individual de los seres humanos. Los retos son continuos, imparables, y en esto el Derecho tiene la difícil obligación de ampararnos y de hacerlo a tiempo, pero bien.

Nos dice el artículo 18.4 de la Constitución Española de 1978 que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Pues bien, más de 40 años después sabemos perfectamente que esto aún es así, y que el futuro nos traerá muchas más muchas situaciones diferentes donde seguirá siendo aplicable. Situaciones que, si bien somos incapaces de prever hoy, de ninguna manera han de suponer que las asumamos como inalcanzables (jurídicamente) hasta grados extremos de la prohibición por temor lo desconocido. Las normas de orden deben ser precisas, proporcionadas y llegar a tiempo en términos de utilidad (conservación), de manera que para su elaboración tengamos en cuenta la experiencia práctica de los

productos y servicios que nos hacen hoy digitales, y que no olvidemos ya se exige sean éticos desde el diseño.

Las empresas e individuos que producen tecnología también tienen responsabilidad en el futuro legal del negocio. Tienen la obligación de ofrecer su actividad bajo criterios de no maleficencia, de respeto a ese artículo 18.4 de la CE y al resto del ordenamiento interno e internacional que le sea aplicable. Allí dónde aún no haya llegado la ley, debe promoverse la autorregulación sobre principios éticos y sobre los límites diseñados por el contenido esencial de los derechos humanos. El Internet de las Cosas, las redes sociales, la banca online, el comercio electrónico, el teletrabajo, las plataformas de contenidos y entretenimiento, la inteligencia artificial. Su mal uso conlleva perjuicios frente al ser humano, y por tanto ha de conllevar responsabilidad legal y/o patrimonial. En ocasiones el daño podrá ser reparado, en ocasiones solo podrá ser indemnizado, y en ocasiones no podrá hacerse nada. La seguridad perfecta y la confianza digital no existen, pero se puede combatir todo aquello que la amenaza con instrumentos técnicos y con instrumentos de concienciación. En último lugar, sin duda, tendremos que poder recurrir a instrumentos de responsabilidad jurídica.

Ofelia Tejerina.
Coordinadora de este título.

Marta Beltrán.
Coordinadora de la colección.

PREFACIO

El Derecho debe asumir la tarea de proteger a las personas físicas y jurídicas frente al mal uso de las tecnologías. Las actividades ilícitas cometidas en el ciberespacio generalmente buscan objetivos económicos, pero pueden también llegar a provocar perjuicios personales de muy difícil reparación. Implantar medidas de seguridad para proteger nuestros activos incluye también conocer, cumplir y aplicar las medidas de carácter legal que ofrece el Estado de Derecho. Con su aprobación y/o su correcta adaptación a este medio se pueden prevenir muchos daños, y si no, se puede al menos intentar su reparación y/o indemnización. Hoy en día es imprescindible conocer las directrices jurídicas que ordenan las relaciones personales, sociales, mercantiles, etc. en el mundo ciber, ya seas técnico o no, para poder actuar respetando sus límites y, en su caso, poder reclamar derechos ante las instituciones competentes.

Los autores que participan en esta obra, juristas de reconocido prestigio y con amplio conocimiento en la materia, aportan al lector una visión multidisciplinar de los principales retos y problemas legales con los que se están encontrando en el contexto de la ciberseguridad. Cuestiones todas ellas que no solo afectan a la vida profesional o de la empresa, sino también a la vida particular de todos y cada uno de nosotros.

Este libro se divide en cinco capítulos, y estos a su vez en diferentes subapartados que han sido seleccionados y organizados por su interés, coherentes al perfil de cada escritor involucrado: ingenieros, abogados, docentes y autoridad policial.

El primer capítulo trata sobre la "seguridad de la información" y cuenta con un primer apartado dedicado expresamente a describir qué significa ética y jurídicamente ser un *hacker*. Qué límites nunca se han de sobrepasarse y cuál

es el fin último del trabajo de un experto en ciberseguridad. En segundo lugar, se invita a conocer cuáles son los ciberdelitos recogidos por el Código Penal y cómo se gestiona su persecución desde el ámbito de la investigación policial. Algo que va intrínsecamente relacionado con el tercer subapartado, dedicado al complicado mundo de las evidencias electrónicas, de las pruebas periciales que debe realizar un forense informático en el curso de una investigación, con el presumible objetivo de ser aportadas en juicio. El cuarto subapartado expone los aspectos más relevantes de la conocida como "Directiva NIS", conscientes de que la alteración de las redes y sistemas de información "pueden generar pérdidas financieras, menoscabar la confianza de la población y, en definitiva, causar graves daños a la economía y a la sociedad, con la posibilidad de afectar a la propia seguridad nacional en la peor de las hipótesis", como señala la propia Exposición de Motivos de la norma que transpuso la Directiva al Derecho interno, el Real Decreto-ley 12/2018, de 7 de septiembre.

El segundo capítulo se ha dedicado por entero a desgranar la normativa vigente sobre protección de datos de carácter personal, en especial en España y Europa, a raíz de la aprobación del famoso RGPD, y ello tanto desde la perspectiva de los derechos de los individuos como desde la perspectiva de la seguridad física y técnica. El daño y las sanciones son los grandes temores de la Sociedad de la Información en esta materia. No cabe duda de que una de las principales preocupaciones del mal uso de las tecnologías hoy en día son los ciberataques y las brechas de seguridad, y más aún, cuando si provocar lesiones en un derecho fundamental que afecta a distintas facetas de nuestra vida privada.

El tercer capítulo se ha dedicado al estudio de los derechos digitales de las personas. En él se expone una inicial reflexión jurídica sobre qué significa tener identidad digital en Internet hoy, que tenemos casi omnipresencia en las redes pero que también que utilizamos la tecnología como medio identificativo. Además, se incluye un subapartado específico sobre los problemas derivados de la presencia online de los menores. Cómo educar y protegerles en sus derechos, para prevenir un futuro digital que no les perjudique su desarrollo personal y profesional. En el siguiente subapartado se reflexiona sobre cómo (ellos, y los adultos) nos expresamos en la red, cómo nos informamos, quiénes son los responsables de que lo podamos hacer libremente y de evitar que nos "infoxiquen" o nos manipulen con contenidos dañinos. Es otro de los aspectos más relevantes de la actualidad y la tecnología, cuya relevancia jurídica se ha puesto de manifiesto a través del término "fake news" o, el más correcto, "desinformación". Por último, se cierra este capítulo con completo estudio de la huella digital que abandonamos online al morir, qué representa para los herederos y qué derechos pueden proteger esa información que nos identificaba o reflejaba la vida que dejaremos.

En el cuarto capítulo se plantean las implicaciones jurídicas más técnicas. Un primer subapartado aborda la protección del software, cómo y de qué manera la propiedad intelectual y la propiedad industrial están al servicio de los creadores y productores. También se analiza en este sentido el futuro de la robótica y la inteligencia artificial en el segundo subapartado, y añade lo correspondiente a las responsabilidades legales y las sanciones que se pueden llegar a imponer por los daños que con su uso se produzcan. Conectando elementos, conectando cosas e Internet, se exponen también, en un tercer subapartado, los retos de la seguridad, técnica y de resultado legal en la compleja interrelación que plantean todos los dispositivos que hoy comunicamos entre sí para (supuestamente) hacernos la vida un poco más cómoda, pero también menos privada. Finalmente, el cuarto subapartado nos lleva a analizar las implicaciones del intercambio de monedas virtuales, blockchain y la seguridad fiscal de las criptomonedas a juicio.

Por último, el quinto capítulo nos deja para un broche de calado internacional. En él se hace un completo e interesantísimo repaso a los retos legislativos a los que se enfrentan desde Latinoamérica en materia de ciberseguridad.

Ofelia Tejerina
Madrid, junio 2020