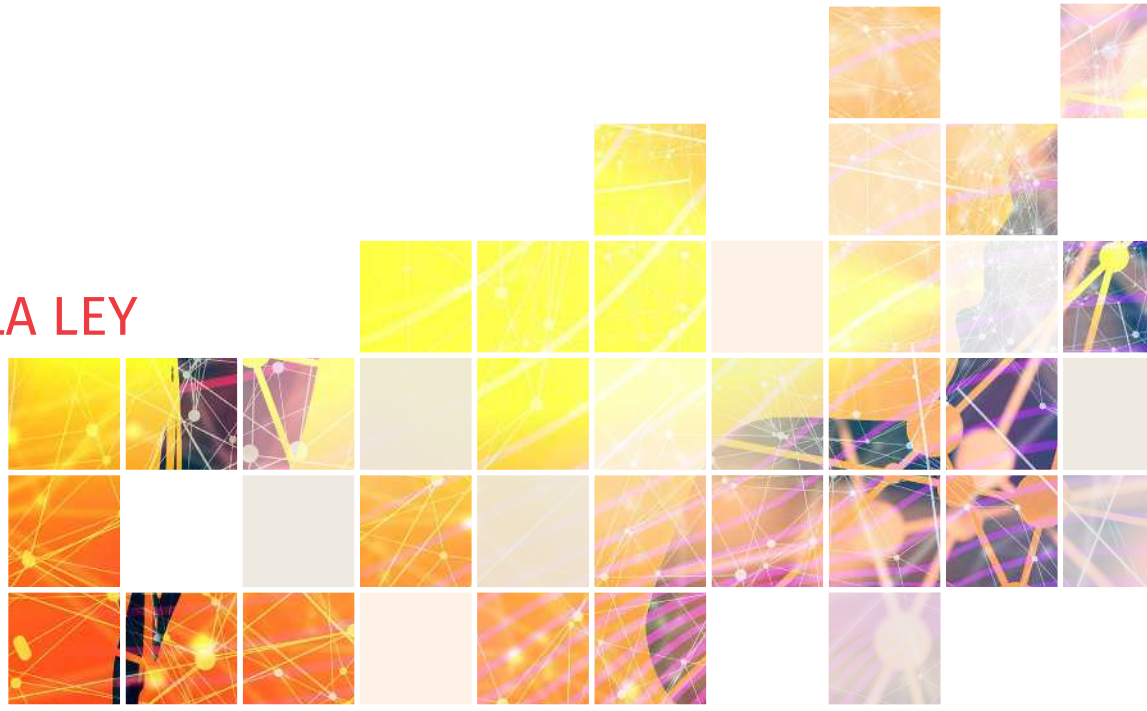
TEMAS

Delitos tecnológicos

Cuestiones penales y procesales

Eloy Velasco Núñez



LA LEY

Wolters Kluwer

TEMAS

LA LEY

Delitos tecnológicos

Cuestiones penales y procesales

Eloy Velasco Núñez

Wolters Kluwer

© **Eloy Velasco Núñez**, 2021
© **Wolters Kluwer España, S.A.**

Wolters Kluwer
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 91 602 01 82
e-mail: clienteslaley@wolterskluwer.es
http://www.wolterskluwer.es

Primera edición: Mayo 2021

Depósito Legal: M-13797-2021
ISBN versión impresa: 978-84-18662-32-4
ISBN versión electrónica: 978-84-18662-33-1

Diseño, Preimpresión e Impresión: Wolters Kluwer España, S.A.
Printed in Spain

© **Wolters Kluwer España, S.A.** Todos los derechos reservados. A los efectos del art. 32 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, Wolters Kluwer España, S.A., se opone expresamente a cualquier utilización del contenido de esta publicación sin su expresa autorización, lo cual incluye especialmente cualquier reproducción, modificación, registro, copia, explotación, distribución, comunicación, transmisión, envío, reutilización, publicación, tratamiento o cualquier otra utilización total o parcial en cualquier modo, medio o formato de esta publicación.
Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la Ley. Diríjase a **Cedro** (Centro Español de Derechos Reprográficos, **www.cedro.org**) si necesita fotocopiar o escanear algún fragmento de esta obra.
El editor y los autores no aceptarán responsabilidades por las posibles consecuencias ocasionadas a las personas naturales o jurídicas que actúen o dejen de actuar como resultado de alguna información contenida en esta publicación.
WOLTERS KLUWER no será responsable de las opiniones vertidas por los autores de los contenidos, así como en foros, chats, u cualesquiera otras herramientas de participación. Igualmente, WOLTERS KLUWER se exime de las posibles vulneraciones de derechos de propiedad intelectual y que sean imputables a dichos autores.
WOLTERS KLUWER queda eximida de cualquier responsabilidad por los daños y perjuicios de toda naturaleza que puedan deberse a la falta de veracidad, exactitud, exhaustividad y/o actualidad de los contenidos transmitidos, difundidos, almacenados, puestos a disposición o recibidos, obtenidos o a los que se haya accedido a través de sus PRODUCTOS. Ni tampoco por los Contenidos prestados u ofertados por terceras personas o entidades.
WOLTERS KLUWER se reserva el derecho de eliminación de aquellos contenidos que resulten inveraces, inexactos y contrarios a la ley, la moral, el orden público y las buenas costumbres.
Nota de la Editorial: El texto de las resoluciones judiciales contenido en las publicaciones y productos de **Wolters Kluwer España, S.A.**, es suministrado por el Centro de Documentación Judicial del Consejo General del Poder Judicial (Cendoj), excepto aquellas que puntualmente nos han sido proporcionadas por parte de los gabinetes de comunicación de los órganos judiciales colegiados. El Cendoj es el único organismo legalmente facultado para la recopilación de dichas resoluciones. El tratamiento de los datos de carácter personal contenidos en dichas resoluciones es realizado directamente por el citado organismo, desde julio de 2003, con sus propios criterios en cumplimiento de la normativa vigente sobre el particular, siendo por tanto de su exclusiva responsabilidad cualquier error o incidencia en esta materia.

Y el tercero, la **suplantación** de la importante labor social de garantía y protección del derecho fundamental a la protección del dato que ejerce **el Juez**, a quien el particular suplanta y sustituye sin justificación —sin legitimidad, formación profesional…— cuando, por no operar circunstancias de urgencia o imposibilidad, su intervención predictiva y pre constitutiva de prueba de datos se podía haber analizado y autorizado o no perfectamente por el propio Juez.

Es decir, excluyendo las situaciones en que la captación del dato personal incriminatorio hecha por tercero obedece a circunstancias de **urgencia** amparadas por la **buena fe** —pues no se podía acudir al Juez a que las autorice, STS 793/2013, de 28 de octubre y 45/2014, de 7 de febrero— o a situaciones en que por anunciadas correctamente —de ahí la importancia de pre informar que se van a captar, grabar o filmar datos— no obedecen a expectativas razonables de privacidad que justifiquen la lesión de la autodeterminación sobre el dato personal afectada —*v. gr.*: STS 489/2018, de 23 de octubre— y a las expresamente conocidas y consentidas por el afectado.

Y el peligro para el derecho fundamental a la protección del dato personal y la autodeterminación informativa se multiplica en los riesgos que supone captar en dispositivos técnicos —de fácil reproducción, alta difusión y cesión a terceros— datos personales de signo incriminatorio, según el destino que se les acabe dando, pero singularmente, tanto el riesgo que genera almacenarlos, como el de difundirlos o divulgarlos a terceros, sin olvidar el de destruirlos cuando ya no cumplan su fin, cuando sea cierto que se captan para **servir de futura prueba**, y con la sola intención de cederlo al Juez —pues no existe norma que establezca la diferencia entre un período de almacenaje razonable hasta cederlo al Juez, y un período en el que sospechar que tal cesión no es, en realidad, la razón por la que un particular ha captado los datos—.

La **conservación de datos personales tecnologizados** con potencialidad incriminatoria también está sujeta a finalidades profesionales y sometida en cuanto a su futura cesión a autorización judicial previa (Art. 6 Ley 25/2007, de 18 de octubre, de conservación de datos y Arts. 39-44 Ley 9/2014, de 9 de mayo, General de Telecomunicaciones), excluyéndose la conservación preventiva masiva e indiscriminada de los mismos basada en límites exclusivamente temporales (*v. gr.*: STJUE Gran Sala de 8 de abril de 2014, caso Digital Rights Ireland C-293/12 y C-594/12, STJUE Gran Sala de 21 de diciembre de 2016, caso Tele2 Sverige AB C-203715 y C-698/15, STJUE de 6 de octubre de 2020, asunto La Quadrature du Net y otros, C-511/18,

C-512/18 y C-520/18 y STJUE Gran Sala de 2 de marzo de 2021, caso HK vs Prokuratuur C-746/18) si no están, como en el caso español, reforzados por más garantías (STS 470/2015, de 7 de julio, STS 768/2015, de 23 de noviembre, STS 272/2017, de 18 de abril, STS 400/2017, de 1 de junio y STS 723/2018, de 23 de enero de 2019), entre las que la de su judicialización, deviene fundamental.

La **finalidad profesional** es también la razón que permite y valida la conservación de datos personales y su cesión y tratamiento en materias importantes para tareas instrumentales de procesos que podrían ser penales, o si no humanitarios, muy relacionados, como son, además de la persecución de delitos, en el caso de la base de datos policial de ADN, los de (Art. 1 LO 10/2007, de 8 de octubre) «*identificación de restos cadavéricos o de averiguación de personas desaparecidas*».

En consecuencia, que un particular, sin finalidad profesional necesaria, se arrogue —y auto otorgue a sí mismo— el derecho a conservar datos personales ajenos captados subrepticiamente sin autorización tanto de su titular afectado, como del Juez, —excluido que la conservación sea compatible con circunstancias de urgencia, pues conservar y urgencia son términos contradictorios entre sí— que no tengan una justificación profesional o social —un dato concreto, para poder preservar funciones ínsitas en determinadas profesiones, que lo justifiquen—, deriva en ilicitudes probatorias, por afectar al derecho protegido en el art. 18.4 CE. Sanción procesal que igualmente debe predicarse de su posterior cesión, que, además, puede también devenir en un delito de revelación de secretos de los Arts. 197.3 ó 7 CP.

Como señala la STJUE Gran Sala de 21 de diciembre de 2016, caso Tele2 Sverige AB C-203715 y C-698/15, sólo el objetivo de la lucha contra la delincuencia grave justifica el acceso a datos personales «*de cuyo conjunto se extraigan conclusiones precisas sobre la vida privada de las personas cuyos datos han sido conservados*», lo que conlleva entender que no es finalidad del ciudadano particular adoptar roles probatorios anticipados ni predictivos —y si en un caso concreto le afectan, por estar siendo víctima de un delito, deberá acudir al Juez, Fiscal o Cuerpo policial oportuno a permitir que estos encarnen esos roles—.

Y como añade la STJUE Gran Sala de 2 de marzo de 2021, caso HK vs Prokuratuur C-746/18, la conservación de datos (en el caso, realizada por prestadores de servicios de comunicaciones electrónicas, sobre datos de tráfico o de localización que puedadn facilitar información sobre las comuni-

caciones efectuadas por el usuario de un medio de comunicación electrónica o sobre la localización de los equipos terminales que utilice) al suponer una injerencia en los derechos fundamentales de los Arts. 7 (respeto a la vida privada y familiar) y 8 (protección de datos de carácter personal) de la Carta de derechos de la Unión Europea, al permitir extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se han conservado —hábitos de vida cotidiana, lugares de residencia permanentes o temporales, desplazamientos diarios, actividades realizadas, relaciones sociales y círculos relacionales que frecuentan—, sólo es tolerable cuando su acceso tenga como objeto fines sociales tan importantes —e impropios de los particulares— como la lucha contra la delincuencia grave o la prevención de amenazas graves contra la seguridad pública.

Vivimos en una sociedad que pretende controlar y conjurar riesgos, para evitar lesiones a bienes jurídicos protegidos prominentes, pero paradójicamente, si para hacerlo, almacenamos y tratamos datos personales prospectiva o predictivamente, generamos otras nuevas lesiones, igualmente denostables, que, al formar parte del problema, deben tenerse en cuenta a la hora de pretender hallar su solución.

En lo que hace a la **cesión del dato personal** —por parte normalmente de las empresas gestoras de servicios telecomunicativos y de Internet, a las que hay que añadir las gestoras de bases de datos personales— con fines probatorios en el proceso penal, cuando no se cuenta con autorización del afectado ni del Juez, la jurisprudencia determina la validez o no de la misma —lo que supone la lesión o no del derecho protegido en el Art. 18.4 CE, que es un derecho fundamental no ilimitado— en función de la **naturaleza y alcance de la injerencia** al mismo, su **proporcionalidad**, pues no afecta igual al derecho que analizamos una injerencia leve que una grave (STJUE, Gran Sala, de 2 de octubre de 2018, C-207/16).

Y así, aunque se afecte el derecho protegido en el Art. 18.4 CE a la hora de investigar delitos, estaría justificada la limitación o sacrificio de su protección, en función de la proporcionalidad, de manera que cuanto más grave sea su injerencia, más grave debe ser el delito que se esté persiguiendo, indicando la referida sentencia que tienen la consideración de **inmisiones graves** —númerus *apertus*— en el derecho a la protección del dato, los siguientes:

– la fecha, hora, duración o destinatarios de las comunicaciones mantenidas con un teléfono,

– la geolocalización, lugares desde donde se han mantenido, o

– la frecuencia de las telecomunicaciones mantenidas con determinadas personas.

Y en general, como apuntaba la citada STJUE Gran Sala de 21 de diciembre de 2016, caso Tele2 Sverige AB C-203715 y C-698/15, aquellas inmisiones que aporten información que permita extraer «*conclusiones precisas sobre la vida privada de las personas*» cuyos datos hayan sido conservados.

No lo es, por su levedad, según el supuesto fáctico analizado en la STJUE Gran Sala de 2 de octubre de 2018 (C-207/16), la solicitud policial a la Operadora telefónica de datos de tarjetas SIM asociados a un teléfono móvil recién robado a su titular de los 12 días siguientes al robo: titularidad de la tarjeta SIM incorporada y el nombre, apellido y dirección de quien la haya introducido tras la sustracción, pues a la levedad de la injerencia en el derecho a la protección del dato, se añade que no son de contenido, al pedirse meramente datos de tarificación.

5.3.4.5. Bases de datos/ficheros. Análisis de datos en la investigación penal. Cruce de datos. Incorporación del dato personal al proceso penal. Destrucción/eliminación del dato penal

Reflexión añadida merece la figura de lo que se conoce como **bases de datos o ficheros**, que el Art. 4.6 RGPD (igual que el Art. 3.6 Directiva 2016/680) define como «*todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica*», por la relación que, conforme al Art. 2.2 de la Directiva 2016/680, tiene con los datos automatizados, que, se refieren, no sólo a los personales que se tratan total o parcialmente de manera automatizada, sino igualmente a los que no, siempre que estén contenidos o destinados a ser incluidos en un fichero.

La experiencia sobre los regulados por la LO 10/2007, de 8 de octubre, en la base de datos policial sobre identificadores obtenidos a partir del ADN, puede servir inicialmente de guía para otras **bases de datos que pretendan el fin público de permitir investigaciones por delito**: el acopio y conservación del dato personal se puede hacer por los cuerpos policiales (Art.1 y 6) y su análisis lo llevan a cabo profesionales acreditados (Art. 5), siempre teniendo en cuenta la finalidad del mismo, que es, principalmente[91] la de permitir la identificación de autores de delitos graves (Art. 3).

(91) Además de para investigar los delitos que describe en el Art. 3.1 a), permite su uso también para identificar cadáveres o investigar la desaparición de personas.

DELITOS TECNOLÓGICOS: CUESTIONES PENALES Y PROCESALES, por un lado, ofrece un detallado estudio de los diferentes delitos tecnológicos (descubrimiento y revelación de secretos, daños y estafas informáticas, contra la propiedad intelectual, pornografía infantil, *phishing*, *sexting*, *grooming*, *stalking*, *cracking*, *spoofing*, injurias y amenazas informáticas, ciberodio, ciberterrorismo...), con sus características, elementos conformadores, circunstancias modificativas propias y la jurisprudencia más reciente sobre los mismos. Y, por otro, aborda en profundidad los aspectos procesales ligados a la investigación tecnológica de este tipo de delitos (ubicuidad, universalidad...), con especial incidencia en la obtención (redes, terminales y dispositivos) y licitud probatoria tecnológica; aseguramiento (clonado y volcado de información, desprecinto); cadena de custodia; instrumentos tecnológicos para su averiguación; interceptación de telecomunicaciones; acceso, uso y análisis de datos; micrófonos; cámaras ocultas; geolocalizadores; filmaciones; tecnovigilancias; registros directos o remotos de dispositivos con información; monitorizaciones; agentes encubiertos virtuales; *blockchain*; artificios de inteligencia artificial; pericial tecnológica; etc.

El libro concluye con el estudio de las medidas restrictivas tecnológicas (retirada de contenidos, interrupción de servicios informáticos e interdicción del acceso), así como las consecuencias accesorias, el análisis de la responsabilidad civil derivada de la delincuencia tecnológica y el marco de cooperación jurídica internacional contra la ciberdelincuencia.

ISBN: 978-84-18662-32-4

AENOR ER-0280/2005 IQNet AENOR GA-2005/0100

Wolters Kluwer