Parlamento Europeo

El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado

Consejo de Europa

ESTUDIO

EPRS | Servicio de Estudios del Parlamento Europeo

Unidad Biblioteca de Derecho Comparado
PE 628.261 – Octubre 2018

ES

EL DERECHO AL RESPETO DE LA VIDA PRIVADA: LOS RETOS DIGITALES, UNA PERSPECTIVA DE DERECHO COMPARADO

Consejo de Europa

ESTUDIO

octubre 2018

Resumen

El presente estudio forma parte de un proyecto más global que pretende poner las bases para poder comparar el régimen jurídico aplicable al derecho al respeto de la vida privada en diferentes ordenamientos jurídicos, así como poder comparar las diferentes soluciones que dichos ordenamientos han previsto para los desafíos que la "era digital" impone a tal derecho.

En las páginas que siguen se estudia, en lo referido al Consejo de Europa y con respecto al tema que nos ocupa, los convenios en vigor, la jurisprudencia más relevante y la naturaleza del derecho al respeto de la vida privada, acabando con unas conclusiones sobre los desafíos mencionados.

AUTOR

El autor de este documento es el **Prof. Dr. Francisco Pérez de los Cobos Orihuel, Presidente Emérito del Tribunal Constitucional de España, Catedrático de la Universidad Complutense de Madrid,** por encargo de la Unidad Biblioteca de Derecho Comparado, Dirección General de Servicios de Estudios Parlamentarios (DG EPRS) de la Secretaría General del Parlamento Europeo.

ADMINISTRADOR RESPONSABLE

Prof. Dr. Ignacio Díez Parra, Jefe de la "Unidad Biblioteca de Derecho Comparado".

Para contactar la Unidad, por favor envíe un correo electrónico a:
EPRS-ComparativeLaw@europarl.europa.eu

VERSIONES LINGÜÍSTICAS

Original: ES

Traducciones: DE, EN, FR, IT

Este documento está disponible en la siguiente dirección de Internet: http://www.europarl.europa.eu/thinktank

CLÁUSULA DE EXENCIÓN DE RESPONSABILIDAD

Manuscrito completado en agosto de 2018

Bruselas, © Unión Europea, 2018

PE 628.261

Impreso	ISBN: 978-92-846-4049-2	DOI:10.2861/539638	QA-04-18-867-ES-C
PDF	ISBN: 978-92-846-4040-9	DOI:10.2861/72951	QA-04-18-867-ES-N

Índice

Lista de abreviaturas

art.	artículo
c.	contra
cit.	citado
Cfr.	Confrontar
CEDH	Convenio europeo para la protección de los derechos Humanos y de las libertades fundamentales
Convenio 108	Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal
nº	número
p.	página
ss.	siguientes
ST.	sentencia
TEDH	Tribunal Europeo de Derechos Humanos
vgr.	verbigracia

Síntesis

El presente estudio aborda el derecho al respeto de la vida privada y los principales retos en la era digital desde la perspectiva del Consejo de Europa. Dicho análisis gira principalmente en torno al artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales que reconoce el derecho de toda persona "al respeto de su vida privada y familiar, de su domicilio y correspondencia", pero se aborda desde una dimensión eminentemente jurisprudencial, en la medida en que, dada la relativa parquedad del CEDH, el Tribunal Europeo de Derechos Humanos ha llevado a cabo una tarea de precisión y delimitación de la extensión y significado de este derecho. Una labor interpretativa del Tribunal de Estrasburgo que además tiene la virtualidad de haber adaptado el contenido del derecho a las nuevas necesidades y contextos.

Partiendo de lo anterior, el estudio se inicia con una breve reseña histórica del marco normativo de referencia, que se configura básicamente a través de dos normas. Por un lado, el ya citado CEDH, con una mención especial, dentro de su vocación eminentemente jurisdiccional, al recurso individual de los particulares ante el TEDH, dado que tal posibilidad fue una primicia desde el punto de vista del Derecho Internacional. Por otro lado, el Convenio nº 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, pues, aunque no tiene eficacia directa en los Estados firmantes ni otorga derechos tutelables ante el TEDH, tiene el indudable valor de haber sido el primer instrumento internacional jurídicamente vinculante en materia de protección de datos personales, además de haber influido muy significativamente en la normativa de la Unión Europea. A lo que se añade su aspiración no meramente europea, en la medida en que está abierto a la adhesión de Estados no miembros del Consejo de Europa y, de hecho, ya se han producido varias adhesiones en tal sentido. Algo particularmente relevante, desde el momento en que uno de los grandes desafíos para el derecho al respeto de la vida privada frente a la digitalización, pasa por la creación de criterios uniformes a nivel internacional que amparen la privacidad frente a las nuevas tecnologías que desdibujan cualquier frontera.

En este sentido, la parte introductoria del estudio también da cuenta sucinta de algunos de los principales desafíos para el derecho al respeto de la vida privada en la era digital, que, de forma resumida, son tres. Primero, hay que restablecer el equilibrio entre las grandes operadoras de internet y los usuarios, para garantizar que éstos últimos mantienen el control sobre sus datos personales. En segundo lugar, otro desafío pasa por proteger la privacidad del ciudadano frente a la renovada capacidad intrusiva de los Estados en nombre de la seguridad colectiva, en la medida en que gracias a los avances tecnológicos en el campo de las telecomunicaciones y del tratamiento de datos es posible una vigilancia secreta a gran escala. Por último, como se apuntaba antes, dado que la red no entiende de fronteras, se hace preciso un marco legal lo más armonizado posible, que ofrezca una protección en materia de protección de datos similar a todos los ciudadanos independientemente del país en que se encuentren.

En la parte central del estudio se analiza el alcance del derecho al respeto a la vida privada en los convenios del Consejo de Europa desde una doble perspectiva. Por una parte, una visión panorámica de las manifestaciones del derecho a la vida privada, con particular atención a las más implicadas por los efectos de las nuevas tecnologías y la digitación, pues, más allá de la enunciación más o menos vaga de los cuatro aspectos del derecho *ex* art. 8 del CEDH –vida privada, vida familiar, domicilio y correspondencia–, el TEDH ha realizado una labor interpretativa que ha venido a cubrir situaciones muy probablemente no previstas por los padres del CEDH. Una interpretación extensiva y generosa por parte del TEDH que también se aprecia desde la perspectiva de las obligaciones para los Estados, en tanto que, como se verá,

no sólo deben abstenerse de cometer injerencias arbitrarias en los ámbitos de la esfera privada del individuo, sino además tienen que actuar para que los ciudadanos disfruten efectivamente de ese derecho y para protegerlos frente a las actuaciones de terceros. Unas obligaciones positivas para los Estados que, desde otra perspectiva, confirma que el derecho a la vida privada del art. 8 del CEDH despliega un "efecto horizontal". A la panorámica general sobre el concepto y alcance del derecho desde el punto de vista de la jurisprudencia del TEDH, se le une una descripción de los principales contenidos sustantivos del citado Convenio 108 en materia de protección de datos personales, que precisamente ha sido objeto de reforma muy recientemente con vistas a dar respuesta al nuevo contexto de la era digital. La parte central del estudio se cierra con una reseña individualizada de algunas de las sentencias más relevantes de la jurisprudencia reciente del TEDH, seleccionadas en función de los aspectos de mayor actualidad desde el punto de vista del objeto del estudio –videovigilancia, geolocalización, vigilancia secreta masiva, derecho al olvido, etc.–.

La tercera parte del estudio se dedica a poner de relieve que el derecho la vida privada *ex* art. 8 CEDH no es un derecho absoluto, pues el propio apartado 2 se encarga de precisar las condiciones que pueden justificar una injerencia por parte de las autoridades –"prevista por la ley", para fines legítimos y que sea "necesaria en una sociedad democrática"–. Por ello, se esboza una descripción general del test utilizado por el TEDH a la hora de enjuiciar la legitimidad de las injerencias, sin perjuicio de las modulaciones o matizaciones que el test puede sufrir respecto a cada materia o caso concreto. A lo que se añade una mención especial a otras limitaciones que particularmente experimenta el derecho a la vida privada en virtud de otros de determinados derechos de terceros.

El estudio finaliza con unas conclusiones sobre la idoneidad de la protección del derecho a la vida privada desde la perspectiva del Consejo de Europa para hacer frente a los principales desafíos puestos de relieve en la introducción del estudio. La conclusión general es que el marco normativo del Consejo de Europa responde adecuadamente a tales desafíos, sin perjuicio de que, en función de los aspectos concretos y considerando la dimensión supranacional de las pautas establecidas, para que tales pautas operen como garantías efectivas de los derechos de los ciudadanos se requiere, sin duda, una actuación legislativa de los Estados. Una legislación que no solo debe operar como garantía de los ciudadanos sino que se presenta como el cauce indispensable para que los propios Estados puedan utilizar las excepciones legítimas al derecho a la vida privada para proteger los intereses generales. Asimismo, del grado de adhesión y seguimiento de las pautas establecidas por el sistema de europeo de derechos humanos dependerá, en gran medida, que se alcance una cierta armonización, especialmente relevante para la materia objeto de estudio, obteniendo una respuesta equilibrada al desafío que la extraterritorialidad plantea para la vida privada en la era digital.

I. Introducción

I.1. El Convenio para la protección de los derechos humanos y de las libertades fundamentales

Cuando el 25 de Agosto de 1950 la Asamblea Parlamentaria del Consejo de Europa aprobó el Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales (CEDH) –entrada en vigor en 1953–, dio carta de naturaleza a un original y ambicioso sistema de protección de los derechos humanos, cuyo verdadero alcance solo su implementación en el tiempo ha permitido desvelar. En un contexto histórico en que eran palpables las nefastas consecuencias de las guerras entre naciones y de los regímenes totalitarios, la firma del CEDH respondió a la voluntad de los fundadores del Consejo de Europa de seguir avanzando en la garantía colectiva de algunos derechos ya anunciados en la Declaración Universal de Derechos Humanos de 1948, como derechos intrínsecos a la dignidad humana y como base de la justicia y la paz en el mundo. Sobre la base de una concepción comunitaria de tales derechos y del patrimonio de ideales compartidos por los Estados Europeos en torno al concepto de democracia, el convenio pretende, en efecto, dar un paso más en la protección de tales derechos. En este sentido, se ha apuntado que la Declaración sería el pacto general de ámbito universal y el CEDH sería el pacto especial regional, ampliado, desarrollado y con unos mecanismos dirigidos al efectivo cumplimiento de los compromisos adquiridos por los Estados en cuanto al respeto de tales derechos, no quedando, además, los mismos condicionados por el principio de reciprocidad entre Estados (Casadevall, 2012, p. 34).

Y entre los derechos incluidos, desde el inicio, en el Convenio se encuentra el derecho de toda persona "al respeto de su vida privada y familiar, de su domicilio y de su correspondencia" (art. 8.1). Se siguió con ello, ciertamente, la estela de la Declaración Universal de Derechos Humanos (art. 12), siendo, asimismo, el reconocimiento de este derecho pauta común en otros textos internacionales en materia de derechos fundamentales (Pacto Internacional de Derechos Civiles y Políticos de 1966 –art. 17–; Convención sobre los Derechos del Niño de 1989 –art. 16–; Carta de Derechos Fundamentales de la Unión Europea de 2000 –art. 7–). Catalogado habitualmente, junto con otros derechos civiles y políticos, como un derecho humano de primera generación, desde hace tiempo se viene coincidiendo en que su reconocimiento internacional ha tenido una notable virtualidad expansiva ante fenómenos tales como el creciente control social en manos de los Estados a partir de la segunda mitad del siglo XX como consecuencia del desarrollo de la capacidad tecnológica (Arzoz, 2009, p. 5 y 6). De hecho, ya desde los primeros casos que fueron enjuiciados por el Tribunal Europeo de Derechos Humanos (TEDH) desde la perspectiva del derecho a la vida privada, el Tribunal tuvo que empezar a delimitar en qué medida los poderes del Estado de controlar las telecomunicaciones pueden interferir en el citado derecho (ST. Klass y otros c. Alemania, 6 septiembre 1978).

Lo anterior permite enlazar con el elemento que más ensalza el valor jurídico de los derechos reconocidos en el CEDH: su protección jurisdiccional. En efecto, entre los mecanismos diseñados por los padres fundadores del Convenio en orden a garantizar la observancia y efectividad de los derechos y libertades que el Convenio declaraba, se introdujo la posibilidad, insólita hasta entonces, de un recurso individual de los particulares afectados ante un órgano jurisdiccional internacional; de suerte que, en adelante, iba a ser factible para los ciudadanos europeos demandar ante un genuino órgano jurisdiccional supranacional a los Estados parte en el Convenio para exigir de ellos el respeto a los derechos fundamentales y libertades

públicas reconocidos en su texto. Desde el punto de vista del Derecho Internacional, la previsión del recurso individual ante el TEDH fue particularmente revolucionaria, pues rompió con el principio según el cual no había más sujetos del Derecho Internacional que los Estados.

El citado recurso individual ha pasado por diferentes fases históricas (Pérez de los Cobos, 2018, p. 15 y ss.): desde una fase inicial en que los Estados parte, a través de diferentes órganos de supervisión del CEDH, ejercían en buena medida un control de tipo político sobre los asuntos que se conocían y sobre la solución dada a los mismos, hasta la actual configuración –para la cual fueron determinantes las reformas introducidas por el Protocolo nº 11 de 1994–, que profundiza en los rasgos jurisdiccionales del sistema y redobla la importancia del recurso individual como pieza central del sistema europeo de derechos humanos y su más genuino signo de identidad. De acuerdo con la actual regulación (arts. 34 y ss. CEDH), cabe afirmar –sin perjuicio de las necesarias matizaciones que se derivan de la concreta configuración del recurso individual– que cualquier persona física, organización no gubernamental o grupo de particulares, sometido a la jurisdicción de un Estado parte del Convenio, que se considere víctima de una violación en su derecho a la vida privada *ex* art. 8 CEDH podrá, tras haber agotado las vías de recursos en el Estado correspondiente, presentar una demanda ante el TEDH, que ejerce su competencia a lo largo de todo el proceso de tutela de los derechos humanos diseñado por el CEDH. Y aunque formalmente la fuerza obligatoria de sus sentencias se predica tan sólo de las partes en litigio, en la práctica las mismas tienen, en buena medida, el papel privilegiado de establecer normas en materia de derechos humanos aplicables en toda Europa (ST. Gaglione y otros c. Italia, 21 diciembre 2010).

I.2. El Convenio 108 sobre protección de datos de carácter personal

La preocupación del Consejo de Europa por el derecho a la vida privada no sólo se ha manifestado a través de los derechos garantizados en el CEDH, sino también a través de otros instrumentos. Desde finales de los años 60, en el seno del Consejo de Europa se suscitó, en efecto, la preocupación por los riesgos que los avances técnicos generan para los derechos humanos, en particular para la vida privada, y se inició una actividad que dio lugar, en los años 70, a la adopción de dos Resoluciones que sentaban algunos principios relativos a la protección de datos personales en el ámbito privado y público. Tales Resoluciones fueron el antecedente del Convenio nº 108 del Consejo de Europa, de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Tal y como se desprende de su Preámbulo y de su art. 1, este instrumento tenía por objeto desarrollar la protección del derecho al respeto a la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de datos personales que son objeto de tratamientos automatizados.

Durante la fase de elaboración de dicho convenio se llegó a poner sobre la mesa la posibilidad de que se enmendase, además, el CEDH para incorporar expresamente la protección de datos de carácter personal al sistema de garantías del mismo (Cfr. Garzón, 1981, p. 15), si bien finalmente el único producto normativo resultante fue el citado Convenio 108. Por tanto, de acuerdo con la regulación contenida en el CEDH (art. 32 y 34), el convenio 108 no otorga derechos tutelables ante el TEDH, al reservarse esta protección para los derechos expresamente incluidos en el Título I del CEDH o en alguno de sus Protocolos adicionales. Y desde el punto de vista de su eficacia en los Estados parte, el Convenio 108 ha sido catalogado como un instrumento *"non self-executing"* (Garzón, 1981, p. 18; Villaverde, 1994, p. 191); esto es, sus efectos vinculantes se despliegan respecto a los Estados firmantes que deben implementarlo y no directamente dentro de los ordenamientos internos. El objeto del convenio es, ciertamente, comprometer a las partes signatarias a incorporar en su derecho

interno las medidas necesarias para hacer efectivos los principios relativos al tratamiento de datos de carácter personal de todos los individuos presentes en su territorio.

Sea como fuere, el principal valor añadido de este convenio es haber sido el primer instrumento internacional jurídicamente vinculante en materia de protección de datos personales. El mismo ha sido ratificado por más de 40 Estados y, por tanto, ha influido muy significativamente en las normativas sobre el particular de la mayoría de Estados europeos y de la propia UE, parte de este convenio a raíz de una enmienda al mismo introducida en 1999. Además, el convenio ha quedado abierto a la adhesión de Estados no miembros del Consejo de Europa (art. 23) y se han producido varias adhesiones en este sentido (Uruguay, Mauricio, Senegal y Túnez). De este modo, puede decirse que el Consejo de Europa fue y sigue siendo un referente a la hora de alertar y adoptar mecanismos respecto a los nuevos desafíos y amenazas que el desarrollo de las nuevas tecnologías comporta para los derechos relativos a la esfera privada de la persona. Esta preocupación del Consejo de Europa queda patente en la continua actividad del mismo en torno a esta materia a través del Comité del convenio, de grupos de trabajo de expertos y de las múltiples Recomendaciones no vinculantes aprobadas que abordan la cuestión del tratamiento de datos en diferentes ámbitos y sectores (Cfr. el sitio web de protección de datos del Consejo de Europa: https://www.coe.int/en/web/data-protection). Todo ello ha permitido, asimismo, encauzar los procesos necesarios para para llegar a acuerdos de reforma del Convenio 108 en dos ocasiones.

De un lado, en 2001 se adoptó un Protocolo adicional al Convenio 108, que introdujo disposiciones sobre los flujos transfronterizos de datos a Estados no parte del convenio y sobre el establecimiento obligatorio de autoridades nacionales de supervisión de protección de datos. Por otra parte, muy recientemente, se ha alcanzado un acuerdo sobre el Protocolo de modificación del Convenio 108 –aprobado por el Comité de Ministros el 18 de mayo de 2018 y abierto a la firma el 25 de junio en Estrasburgo–, que constituye una reforma bastante ambiciosa del texto original y que obedece a la necesidad de responder mejor a los retos para la vida privada que se derivan del uso cada día mayor de las tecnologías de la información y comunicación, la globalización en las operaciones de tratamiento de datos y el flujo cada vez más importante de datos personales. Con esta modernización del convenio se pretenden reafirmar los principios y garantías existentes y se introducen nuevos mecanismos para hacer frente a los riesgos para la privacidad derivados del "mundo on-line" (Cfr. "Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data"). En el epígrafe siguiente se abunda un poco más en los desafíos que el actual desarrollo de las nuevas tecnologías y la llamada digitalización parecen comportar para el derecho a la vida privada y más adelante cuando nos ocupemos de las principales manifestaciones del derecho a la vida privada se reseñarán los contenidos esenciales del actual Convenio 108 (véase *infra* II.3.1.1).

I.3. Desafíos para el derecho a la vida privada en la era digital

En contra de los planteamientos libertarios de algunos de los pioneros de internet, la red no es ni puede ser un territorio ajeno al derecho. Cuando las personas se conectan lo hacen para comunicarse, trabajar, contratar o realizar trámites ante la administración y nada justifica que no dispongan en tal circunstancia de los mismos derechos que cuando están desconectados. Algo primordial si se tiene en cuenta que la misma red, que abre o facilita espacios de la libertad de expresión, podría fragilizar otros derechos, como la vida privada. Porque, aunque resulte paradójico, internet, la gran red descentralizada, libre y sin controles en su origen, podría terminar convirtiéndose en un gigantesco panóptico digital, en el que nadie ni nada escapa al control, dado que subimos a la red todo tipo de información sin saber quién, ni qué, ni cuándo, ni en qué lugar se sabe de uno. Porque ya no figura sólo nuestra edad, género o

profesión, sino que revelamos también nuestros intereses, opiniones, amistades, etc. Un conjunto de datos que se incrementa exponencialmente cuando realizamos transferencias bancarias, reservamos vuelos o hacemos la compra desde el móvil o la tableta. Y que podría ser aún mayor en los próximos años, en la medida en que se desarrolle el denominado internet de las cosas; esto es, datos personales pero generados por sensores y no directamente por la persona, como los que evalúan la productividad en el trabajo, el estado de salud o la calidad del sueño. Al final, nuestros hábitos y rutinas diarias, nuestras relaciones personales, nuestros gustos y toda nuestra vida estará en la red.

Un nivel de divulgación de datos y de exposición pública que podría hacer pensar que en la red desaparece la frontera entre la esfera pública y la esfera privada del individuo y que, por ende, deja de tener sentido el derecho al respeto de la vida privada, pero no es así, porque esos mismos usuarios, cuando se conectan, configuran distintos niveles de privacidad frente a terceros, activan extensiones antirastreo, utilizan servicios de comunicación encriptados o de mensajería efímera u optan por redes sociales cuyos usuarios son anónimos. Es decir, sigue habiendo una cierta aspiración a la privacidad, eso sí, en una dimensión renovada. La idea no es impedir el acceso de otros, sino garantizar que cada sujeto pueda decidir qué información comparte, con quién y el uso que se hace de la misma. Algo primordial si te tiene en cuenta el creciente interés de las entidades públicas y privadas por acceder a toda esa información que subimos o desprendemos cuando nos conectamos.

En unos casos la motivación es económica. Las grandes corporaciones acumulan cantidades ingentes de datos sobre los usuarios de la red en tanto que potenciales consumidores. Ciertamente, antes de que llegara internet las empresas ya explotaban toda la información disponible sobre sus clientes para tratar de optimizar los procesos de producción, mejorar la gestión de sus recursos o lanzar nuevas promociones; la diferencia está en que ahora, gracias al rastro que dejamos en la red, es posible saber qué hacen, qué buscan y, lo más relevante, intuir qué quieren 4.000.000.000 de usuarios de internet. Estamos ante una nueva mercancía, para algunos comparable con el oro o el petróleo en revoluciones económicas anteriores, cuyo valor dependerá de su utilidad para la elaboración de estudios de mercado y perfiles de consumidores (Andrejevic, 2007, p. 81 y ss.). Una valorización de los datos que ha puesto en serio riesgo nuestra esfera privada. Unas veces porque se comercia con nuestros datos sin que ni siquiera lo sepamos. Otras veces porque aceptamos las condiciones de privacidad del sitio web sin tan siquiera leerlas. Se diría que no somos conscientes de los riesgos que entraña la exposición o divulgación de datos personales o que hemos decidido ignorarlos. Y aun en otras ocasiones porque renunciamos a nuestra privacidad a cambio de la gratuidad del servicio, en la medida en que el consentimiento para explotar los datos es condición para acceder al sitio web. ¿De qué sirve leer la política de privacidad si no se tiene posibilidad alguna de modificarla? Sea como fuere, lo cierto es que llevamos años navegando por la red sin conocer o prestar atención a la política de privacidad de los sitios web.

Así que llegados a este punto el primer gran desafío para el derecho a la vida privada en la era digital pasa por devolver al usuario de la red la capacidad real de decidir qué datos quiere compartir, para qué y con quién. Y para ello no basta, como se ha demostrado a lo largo estos años, con reconocer unos derechos en la ley, sino que, antes de nada, hay que sensibilizar a los ciudadanos sobre los riesgos asociados a la divulgación y exposición de sus datos. La labor de divulgación debería empezar en las escuelas y continuar a todos los niveles. Además hay que promover políticas de privacidad más claras y transparentes. Una de las quejas más frecuentes de los usuarios es la excesiva longitud y complejidad de las cláusulas de protección de datos. Un objetivo al que deberían en todo caso contribuir las autoridades de control, las asociaciones de consumidores y usuarios y las grandes plataformas y operadores de la red. El

reto es, en definitiva, avanzar en la garantía del "efecto útil" de la protección de los datos personales.

Otras veces la motivación es político-pública. Nos referimos al interés de los Estados en disponer de información sobre sus ciudadanos. Un interés que es casi tan antiguo como los propios Estados, pues ya en su origen trataron de conocer el número e identidad de los mismos. Ahora bien, una cosa es conocer nuestras opiniones o necesidades para definir prioridades de actuación pública o mejorar los servicios públicos y otra bien distinta vigilar de forma secreta, masiva y preventiva a esos mismos ciudadanos. En este sentido, casi todo el mundo habrá oído hablar del caso Snowden: un exanalista de la CIA que reveló la existencia de PRISM, un programa de la Agencia de Seguridad Norteamericana que, al parecer, permitía captar correos electrónicos, videos, fotografías, llamadas de voz e imagen, actividad en la red, contraseñas y otros datos personales, incluso en el extranjero, contando para ello con la colaboración de las grandes empresas tecnológicas de Estados Unidos y de los servicios secretos de otros países. Existe una *comunnis opinio* –y así lo ha admitido, como se verá, el propio TEDH– sobre la legítima capacidad de los Estados para llevar a cabo una vigilancia secreta en orden a preservar la seguridad nacional y el orden público, si bien –como también tempranamente puso de manifiesto el propio Tribunal de Estrasburgo– ese poder no puede ser arbitrario o ilimitado, pues de lo contrario se corre el riesgo de "destruir la democracia con el motivo de defenderla" (ST. Klass y otros c. Alemania, 6 septiembre 1978). De ahí que el segundo gran desafío pasa por definir hasta dónde y cómo puede vigilar el Estado en pos de la seguridad nacional sin poner en riesgo las mismas libertades que pretende defender. Se trata, en los términos que, como veremos, utiliza el TEDH, de alcanzar un equilibrio justo entre la posibilidad de llevar a cabo una vigilancia secreta que proteja a la sociedad en su conjunto y la necesaria salvaguarda de los derechos individuales de los ciudadanos, en la medida en que no podemos aspirar al cien por cien de seguridad ni al cien por cien de privacidad.

Finalmente, dado que la protección a menudo está circunscrita a un determinado territorio, la circunstancia de que los datos no entiendan de fronteras representa un riesgo añadido para el derecho a la vida privada. La existencia de tantas regulaciones como Estados, a veces muy diferentes, puede plantear importantes conflictos sobre la ley y la jurisdicción aplicable, además de dudas sobre la propia efectividad de la protección para los usuarios. De nada sirve establecer un marco regulador nacional que proteja los derechos si los operadores y las plataformas se encuentran en el extranjero y la ley aplicable es la del país de destino. Un componente de extraterritorialidad que también está presente en los sistemas de vigilancia secreta y a gran escala, dado que a menudo se hace preciso buscar a los terroristas y a los delincuentes más allá de las fronteras nacionales. Lo que plantea a su vez otro interesante conflicto. Esta vez entre el deber y el derecho de un país a defender su seguridad nacional, interceptando comunicaciones en el extranjero, y el deber y el derecho de otro Estado a garantizar el derecho a la vida privada de sus ciudadanos, frente a injerencias de servicios de inteligencia de ese otro Estado. Partiendo de lo anterior, el tercer gran desafío pasa por conseguir una cierta armonización de la protección de los derechos a nivel global, no sólo dentro de Europa sino también con el resto del mundo, de suerte que no sólo se garanticen unos derechos básicos para todos los usuarios de la red, sino que se aporte además la necesaria seguridad jurídica a los operadores, con independencia de dónde estén unos y otros, y legitimidad a las actuaciones de los Estados en su lucha contra el terrorismo, el crimen organizado y otros fenómenos tales como la ciberdelincuencia.

II. El concepto de derecho al respeto de la vida privada en los convenios del Consejo de Europa

II.1. Consideraciones generales

Como se apuntaba anteriormente, el art. 8.1 del CEDH recoge el derecho a la vida privada, disponiendo concretamente que: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia". Por su parte, el apartado 2 del citado artículo 8, de forma similar a lo que ocurre con otros derechos consagrados en el Convenio, se encarga de precisar que: "No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás". Junto a ello hay que volver a mencionar el Convenio 108, que, aunque sin crear nuevos derechos tutelables ante el TEDH, desarrolla e incluye la protección de datos de carácter personal dentro del contenido del derecho al respeto de la vida privada (véase *supra* I.2 e *infra* II.3.1.1). Estas son, por tanto, las dos principales referencias normativas concernientes al derecho a la vida privada dentro del sistema de derechos humanos del Consejo de Europa.

Centrándonos ahora en el CEDH, su morfología responde a las características propias de este tipo de instrumentos internacionales, si bien respecto al citado art. 8 se ha señalado que probablemente nos encontramos ante el derecho más imprecisamente recogido en el texto del Convenio, lo que ha llevado a que su alcance haya quedado extremadamente expuesto a una interpretación judicial muy basada en el caso concreto, algo característico con carácter general de la jurisprudencia del TEDH, pero que quizá también se manifiesta más intensamente en el caso del derecho reconocido en el art. 8 CEDH (Lafferty, 2014, p. 522 y 590). Por consiguiente, a menudo es muy complejo y no resulta prudente extraer conclusiones generales a partir de la lectura de los pronunciamientos del TEDH, pues las circunstancias particulares del caso concreto suelen adquirir tal relevancia en la doctrina formulada, que no es posible hacer una lectura de la misma desligada de tales circunstancias.

Esa indefinición y casuismo no ha sido, sin embargo, óbice para entender que la voluntad de los redactores del Convenio era proteger fuertemente el derecho reconocido en el art. 8 CEDH (Renucci, 2015, p. 229). Y así lo ha entendido TEDH con una doctrina en que la vaguedad conceptual se ha puesto, en buena medida, al servicio de una interpretación generosa y extensiva de tal derecho, dando lugar a que a través del mismo se haya dado protección a situaciones referidas a temas tan diversos como, por ejemplo, la identidad sexual, la protección de datos personales, las relaciones paterno-filiales o las cuestiones medio-ambientales. De hecho, doctrinalmente se coincide en señalar que la jurisprudencia del TEDH relativa al derecho consagrado en el art. 8 constituye una de las manifestaciones más elocuentes de la denominada lectura del Convenio como "instrumento vivo", permitiendo que bajo la protección del art. 8 tenga cabida una gran amplitud de cuestiones en que la idea de vida privada entronca con otros conceptos, asimismo, amplios y difusos, tales como el desarrollo de la personalidad o la autonomía personal, y consintiendo que dicha protección se haya ido adaptando a los profundos cambios sociales y tecnológicos experimentados en las últimas décadas (Cfr. Casadevall, 2012, p. 325; Lafferty, 2014, p. 522, 523 y 530; Sudre, 2015, p. 671).

II.2. Obligaciones negativas y positivas para los Estados

La obligación de los poderes públicos de no cometer injerencias arbitrarias en los ámbitos de la esfera privada del individuo a las que alude el art. 8 del CEDH aparece como la "finalidad esencial" del citado artículo (ST. Kroon y otros c. Países Bajos, 27 octubre1994). Así lo recalca el primer inciso del apartado 2 del precepto –"No podrá haber injerencia de la autoridad pública (…)"–, sin perjuicio de que a continuación el mismo recoja las condiciones que deben darse para poder justificar una injerencia (véase *infra* IV). El CEDH se expresaría, por tanto, en términos clásicos, imponiendo obligaciones negativas o de abstención a los poderes públicos frente al ejercicio del derecho.

Sin embargo, el TEDH no sólo ha perfilado el derecho a la vida privada en términos negativos, sino que reiteradamente se ha pronunciado sobre la obligación de los Estados de actuar para permitir disfrutar efectivamente a los ciudadanos del derecho y también para protegerlo frente a las actuaciones de otros sujetos (entre otras, ST. Marckx c. Bélgica, 13 junio 1979; ST. Jhonston y otros c. Irlanda, 18 diciembre 1986; ST. X e Y contra Países Bajos, 26 marzo 1985; ST. Von Hannover c. Alemania, 24 junio 2004; ST. K.U. c. Finlandia, 2 diciembre 2008). Se entiende, por tanto, que del art. 8 CEDH se derivan inherentemente obligaciones positivas para los Estados.

A este respecto, se ha subrayado que a la hora de precisar el contenido de estas obligaciones positivas y, por tanto, si los Estados han cumplido con las mismas, el TEDH suele aludir al importante margen de apreciación del que disponen los Estados (Lafferty, 2014, p. 523 y 533). La alusión a este margen de apreciación es, en efecto, otra de las notas características de la jurisprudencia del TEDH, que parece darse particularmente respecto a las obligaciones positivas, con fundamento en la mayor cercanía de las autoridades a las circunstancias del conflicto y a la legislación y prácticas nacionales aplicables (ST. Rees c. Reino Unido, 17 octubre 1986; I. c. Reino Unido, 11 julio 2007). En algún supuesto, el TEDH ha llegado incluso a hacer referencia a la no imposición de cargas excesivas a los Estados a la hora de determinar el alcance de las obligaciones positivas (ST. Novoseletskiy c. Ucrania, 22 febrero 2005; ST. Wilson c. Reino Unido, 23 octubre 2012). Con todo, lo cierto es que la afirmación de obligaciones positivas ha ido adquiriendo una importancia creciente en la evolución jurisprudencial del TEDH en torno al derecho a la vida privada (Renucci, 2015, p. 228 y 229).

Visto desde otro ángulo, el reconocimiento de obligaciones positivas confirma que el derecho a la vida privada consagrado en el art. 8 CEDH despliega un "efecto horizontal" (Sudre, 2015, p. 674). Esto es, aunque en el sistema de tutela judicial del CEDH sólo pueden ser demandados los Estados parte (art. 34 CEDH), no admitiéndose, por tanto, las demandas contra particulares, ST. Durini c. Italia, 12 enero 1984), la doctrina del TEDH relativa a la obligación de los Estados de impedir las violaciones realizadas por terceros y proteger al afectado por las mismas comporta de hecho el reconocimiento de la aplicación de los derechos del convenio a las relaciones interprivadas, si bien la responsabilidad última por la violación del derecho cometida por un particular será imputable al Estado por vía de incumplimiento de sus obligaciones positivas. Pronunciamientos recientes del TEDH relativos al respeto de la vida privada de los trabajadores frente al control de sus comunicaciones electrónicas o la videovigilancia llevada a cabo por su empleador son buena muestra de la eficacia horizontal que cabe predicar del derecho reconocido en el art. 8 del Convenio (ST. Barbulescu c. Rumania, 5 septiembre 2017; ST. López Ribalda y otros c. España, 9 enero 2018).

Ahora bien, la alusión a obligaciones positivas por parte del TEDH se viene produciendo en una variedad muy amplia de supuestos: en situaciones en que claramente lo que se le exige a la autoridad es la tutela del derecho frente a las injerencias de terceros, pero también en otras en que la obligación que se predica consiste en la ejecución por parte de las autoridades de

determinados procedimientos o deberes de información para salvaguardar el derecho (véase la clasificación de Grabenwarter, 2014, p. 219 y ss.). De ahí que la distinción entre si en un caso concreto entran en juego las obligaciones negativas o positivas del Estado no sea siempre una distinción fácil. Y, sin embargo, es una distinción *a priori* relevante desde el punto de vista del enfoque a adoptar para la resolución de la cuestión planteada, pues si lo que se pone en duda es el cumplimiento del Estado de sus deberes negativos de no interferir en el derecho, el TEDH procede a verificar, con un enfoque bastante procedimentalizado, si se cumplen o no las condiciones consignadas en el apartado 2 del art. 8 para justificar legítimamente la injerencia en el derecho; mientras que si lo que se valora es el cumplimiento del Estado de sus obligaciones positivas, la decisión pende de una valoración más libre sobre el justo equilibrio entre los intereses en conflicto en el caso concreto (Lafferty, 2014, p. 524 y 532 y ss.). Sin embargo, el propio TEDH, consciente de que la frontera entre las obligaciones positivas y negativas no se presta a una definición precisa, se ha encargado de señalar reiteradamente que los principios aplicables son comparables o similares, particularmente por lo que se refiere a la necesidad de tener en cuenta dicho justo equilibrio entre los intereses del individuo y el interés general y que en ambos casos el Estado goza de un cierto margen de apreciación (entre otras, ST. Keegan c. Irlanda, 26 mayo 1994; ST. Von Hannover c. Alemania, 24 junio 2004; ST. Dickson c. Reino Unido, 4 diciembre 2007; ST. Barbulescu c. Rumania, 5 septiembre 2017).

II.3. Manifestaciones del derecho a la vida privada

El art. 8 CEDH engloba dentro del mismo derecho cuatro aspectos: vida privada, vida familiar, domicilio y correspondencia. Sin embargo, el TEDH, aunque sin negar expresamente la autonomía de tales nociones, parece prescindir de forma bastante deliberada de delimitaciones y precisiones conceptuales y a menudo en los casos enjuiciados se refiere de forma indistinta o superpuesta a los diversos aspectos señalados en el art. 8 del Convenio (Casadevall, 2012, p. 324; Sudre, 2015, p. 676). Además, la invocación de uno u otro aspecto por parte del demandante no parece tener excesivas repercusiones desde el punto de vista del enfoque adoptado por el Tribunal a la hora de valorar si una injerencia pública en el derecho encuentra justificación o no, así como a la hora de determinar si existen obligaciones positivas del Estado (Lafferty, 2014, p. 524).

La citada vaguedad conceptual y vocación expansiva que caracteriza a la jurisprudencia del Tribunal de Estrasburgo en torno al art. 8 CEDH, hacen complejo deducir de la misma una enunciación sistemática y taxativa de las manifestaciones del derecho *ex* art. 8 CEDH. En todo caso, a los fines que aquí interesan, a continuación se realiza una reseña panorámica y no exhaustiva de diversos ámbitos materiales a los cuales se ha extendido la protección brindada por la jurisprudencia del TEDH. Tanto en esta reseña como mediante el próximo epígrafe relativo a algunas sentencias significativas de la jurisprudencia reciente del TEDH (*infra* III), se prestará especial atención a aquellas cuestiones que mejor pueden permitir ver de qué modo la interpretación del art. 8 CEDH se enfrenta o puede enfrentarse a los retos del "mundo digital". Por ello, se va a prescindir de hacer referencia a aquellos aspectos que, a luz de la jurisprudencia del TEDH, quedan encuadrados con mayor autonomía dentro de la noción de "vida familiar" y de "domicilio", tanto porque se apartan de la idea más estricta de privacidad –sobre todo los relativos a la "vida familiar"–, como porque no se ven tan afectados por las implicaciones del desarrollo de las nuevas tecnologías y la digitalización.

II.3.1. Vida privada

Resulta habitual la afirmación contenida en la doctrina del TEDH de que "vida privada" es un término amplio que no se presta a definiciones exhaustivas, no pareciendo apropiado restringir la noción a elementos propios de la esfera más íntima de la persona, tales como

acontecen en torno al domicilio u otras dependencias privadas, despreciando otros aspectos de la identidad y el desarrollo personal de los sujetos y de sus relaciones con los demás (entre otras, ST. Niemietz c. Alemania, 16 diciembre 1992; ST. Pretty c. Reino Unido, 25 abril 2002; ST. Söderman c. Suecia, 12 noviembre de 2013). Sobre la base de estas premisas, los supuestos valorados por el TEDH como una posible violación de la vida privada se refieren a una amplia variedad de situaciones y cuestiones:

- Desde la citada concepción amplia que la jurisprudencia de Estrasburgo ha venido adoptando en cuanto a la noción de vida privada, se ha considerado en diversas ocasiones que la misma engloba la protección de la **integridad física, psíquica y moral** de la persona. Así, la protección del art. 8 CEDH llega a compartir un cierto espacio con la tutela brindada por el art. 3 del mismo Convenio, relativo a la prohibición de la tortura y los tratos inhumanos o degradantes, pudiéndose diferenciar su aplicación en función de la gravedad de la violación, de modo que comportamientos que no revisten la suficiente gravedad para considerarse contrarios al art. 3 CEDH podrían considerarse un atentado a la integridad contraria al art. 8 CEDH (Sudre, 2015, p. 679). Desde esta perspectiva, se ha apreciado una violación de la vida privada cuando, por ejemplo, las autoridades públicas someten a una persona discapacitada y a un familiar suyo a un registro personal desproporcionado respecto a las circunstancias concurrentes, causándoles daños psicológicos (ST. Costello-Roberts c. Reino Unido, 25 marzo 1993). También se ha constatado una violación del art. 8 CEDH cuando las autoridades someten a los sujetos a un tratamiento o intervención médica sin su consentimiento (ST. Y. F. c. Turquía, 22 julio 2003; ST. Glass c. Reino Unido, 9 marzo 2004). Y, en esta misma línea, la protección de la integridad física y moral puede comportar que los Estados asuman la obligación de garantizar las medidas y procedimientos adecuados para que los ciudadanos comprendan y puedan dar un consentimiento suficiente informado sobre las actuaciones médicas a las que se van a someter y recibir **información sobre riesgos para la salud** (ST. Trocellier c. Francia, 5 octubre 2006; ST. Codarcea c. Rumanía, 2 junio 2009). Y es que, con carácter general, el TEDH viene considerando incluida en la protección del art. 8 CEDH todas aquellas situaciones en que la protección de la salud puede quedar vinculada a la existencia de procedimientos adecuados de acceso a información en manos de sujetos públicos o privados (ST. Roche c. Reino Unido, 19 octubre 2005; ST. McGinley y Egan c. Reino Unido, 9 junio de 2008; ST. Vilnes y otros c. Noruega, 5 diciembre 2013).

  Las obligaciones positivas inherentes al respeto a la vida privada que pesan sobre los Estados también comportan que los mismos deben adoptar las medidas penales efectivas para **prevenir y sancionar comportamientos graves entre individuos que afecten a la integridad y vida privada de la persona**, tales como son los que se refieren a la esfera sexual, en especial si conciernen a personas particularmente vulnerables como discapacitados o menores (ST. X e Y contra Países Bajos, 26 marzo 1985; ST. M.C. c. Bulgaria, 4 diciembre 2003; ST. M. C. c. Rumanía, 27 septiembre 2011; ST. Söderman c. Suecia, 12 noviembre de 2013). Estas obligaciones se predican también en aquellos casos en que los desarrollos tecnológicos facilitan la realización y dificultan la persecución de tales delitos, como ocurre cuando se utiliza el anonimato de internet para publicar un anuncio de naturaleza sexual referido a una menor de 12 años. La persecución de este tipo de comportamientos graves se impone por encima de la obligación de determinados sujetos –prestadores de servicios de internet– de guardar la confidencialidad de los usuarios (ST. K. U. c. Finlandia, 2 diciembre 2008).

- Aunque, a diferencia de lo que ocurre en otros textos internacionales, el CEDH no consagra expresamente el **derecho a la reputación**, el TEDH ha cobijado este derecho bajo el art. 8 CEDH en conexión con los límites al derecho a la libertad de expresión *ex* art. 10,

considerándolo un aspecto imbricado en la identidad personal e integridad psicológica que forman parte del derecho a la vida privada (ST. Chauvy y otros c. Francia, 29 junio 2004; ST. Pfeifer c. Austria, 15 noviembre 2007). La doctrina del TEDH se muestra, con todo, bastante exigente a la hora de constatar un ataque a la reputación o al honor contrario al art. 8 CEDH (Lafferty 2014, p. 553), requiriéndose una cierta gravedad del ataque y considerando legítimos aquellos comentarios o expresiones referidas a una persona que tienen un interés general, como elemento que hace prevalecer las libertades de información y expresión (ST. A. c. Noruega, 9 abril 2009; ST. Polanco Torres y Movilla Polanco c. España; 21 septiembre 2010; ST. Mater c. Turquía, 16 julio 2013; ST. Fürst-Pfeifer c. Austria, 17 mayo 2016). No se ha considerado, por ejemplo, una violación del art. 8 CEDH el reportaje periodístico cuyo objeto principal eran las eventuales actividades ilegales de cargos públicos, sin que se apreciase una falta de diligencia periodística en la publicación de las informaciones (ST. Polanco Torres y Movilla Polanco c. España; 21 septiembre 2010). En cambio, sí que se ha considerado una injerencia ilegítima aquel artículo periodístico que apuntaba como probable autor de un delito de violación y asesinato a una persona, sin relevancia pública, a la que simplemente se le había interrogado, junto con otras personas, por la policía (ST. A c. Noruega, 9 abril 2009).

Por lo demás, especial mención merece algún pronunciamiento del TEDH en que se admitió que, en virtud de la tutela que merece la persona frente a los comentarios difamatorios, se pueda condenar como responsable civil a un página web de noticias por los comentarios ofensivos contra una persona realizados por los usuarios en la propia web al hilo de la noticia, sin que tal exigencia de responsabilidad constituya una injerencia ilegítima en la libertad de expresión. Para llegar a tal conclusión el TEDH tomó en consideración factores tales como la mayor difusión que tales comentarios pueden adquirir en un medio digital, la cierta conexión existente entre el artículo publicado y los comentarios de los usuarios y, por tanto, la cierta integración de los primeros en el producto ofrecido al público, así como las menores dificultades, cargas y costes para el medio de comunicación, en comparación con otros sujetos, para controlar lo que se publica en su portal, quien lo publica e impedir conductas ofensivas (ST. Delfi AS c. Estonia, 10 octubre 2013).

- El derecho a la vida privada también se ha revelado idóneo, en ocasiones de forma conjunta con la prohibición de discriminación *ex* art. 14 CEDH, para tutelar los intereses de la persona relacionados con su **libertad e identidad sexual.** Teniendo en cuenta que las tendencias y el comportamiento sexual de las personas son uno de los aspectos más vinculados a la vida privada, se ha considerado que las disposiciones penales de los Estados que castigan las relaciones homosexuales consentidas entre adultos, o que dan un tratamiento diverso y peyorativo en cuanto a la edad establecida para considerar consentidas estas relaciones respecto a las de otra naturaleza, constituyen una injerencia injustificada en la vida privada (ST. Dudgeon c. Reino Unido, 22 octubre 1981; ST. L. y V. c. Austria, 9 enero 2003). Asimismo, la investigación y las sanciones de las autoridades respecto a la tendencia sexual de los miembros de las fuerzas armadas han sido calificadas como una injerencia ilegítima, pues aunque tal actuación de las autoridades pudiera tener cobertura legal, no se entendió que concurriese la necesidad en la persecución de un fin legítimo, en la medida que las tendencias sexuales no se pueden considerar una amenaza para la eficacia y buen funcionamiento de las fuerzas armadas (ST. Lustig-Prean y Beckett c. Reino Unido, 27 septiembre 1999).

  Por otra parte, el TEDH se ha pronunciado en un buen número de ocasiones sobre la transexualidad y, en particular, sobre las obligaciones positivas de los Estados respecto de aquellas personas que solicitan el reconocimiento –por ejemplo, a través de las oportunos

cambios en los registros públicos– de su nueva identidad sexual. La jurisprudencia del TEDH ha experimentado una significativa evolución, pues durante una primera etapa se mostró remisa a establecer pautas concretas desde el punto de vista del art. 8 CEDH, dejando un amplio margen de apreciación a los Estados (ST. Rees c. Reino Unido, 17 octubre 1986; ST. Sheffield y Horsham c. Reino Unido, 30 julio 1998). Sin embargo, posteriormente, con fundamento en la propia doctrina del TEDH que vincula vida privada y desarrollo de la personalidad y en el mayor consenso internacional alcanzado en la materia, ha afirmado claramente la obligación que asumen los Estados de reconocer jurídicamente la nueva identidad de las personas transexuales (ST. Goodwin c. Reino Unido, 11 julio de 2002; ST. Grant c. Reino Unido, 23 mayo 2006).

- Como se apuntaba anteriormente, la vocación expansiva de la noción de vida privada hacia aspectos relacionados con el **desarrollo personal y social** ha llevado a tutelar otras situaciones difícilmente imaginables desde una concepción más clásica de vida privada. Así, el TEDH se ha pronunciado en varias ocasiones sobre las obligaciones que asumen los Estados en torno al **derecho a la persona a conocer sus orígenes**. A este respecto, se ha entendido que el Estado no incumple sus obligaciones positivas cuando no impone a un tercero someterse a análisis de paternidad para satisfacer las pretensiones de otra persona acerca de su paternidad, pero sí las incumple si no dispone de medios alternativos y procedimientos adecuados para encauzar el derecho de toda persona, máxime si es un menor, a conocer la identidad de sus progenitores (ST. Mikulic c. Croacia, 7 febrero 2002). La cuestión se ha planteado en términos similares respecto al acceso a datos personales en manos de las Administraciones (véase *infra II.3.1.1.*). Si la vida privada del tercero no queda comprometida, en tanto que ya fallecido, debe prevalecer el derecho de la persona a conocer sus orígenes, por lo que se considera que la negativa de las autoridades a realizar una pruebas de ADN al difunto viola el art. 8 CEDH (ST. Jaggi c. Suiza, 13 julio 2006).

- Otro gran ámbito de cuestiones que, como se viene apuntando, resulta especialmente relevante desde el punto de vista de las implicaciones de la digitalización, es el relativo a la **protección de datos personales**. En este sentido, el TEDH considera que la protección de datos personales es un aspecto fundamental para el derecho a la vida privada (ST. M. S. c. Suecia, 27 agosto 1997), respecto del que se debe estar, además, especialmente vigilante dados los progresos técnicos de registro y reproducción de datos (ST. Amann c. Suiza, 16 febrero 2000; ST. Rotaru c. Rumania, 5 mayo 2'TEDH+2000+87'000; ST. Peck c. Reino Unido, 28 enero 2003). Dada su relevancia para este estudio, a esta materia se le dedica específicamente un epígrafe posterior (*infra* II.3.1.1), sin perjuicio de que la protección de datos personales también se ve, en mayor o menor medida, implicada en otras cuestiones más particulares –v.gr. videovigilancia, interceptación de las comunicaciones– a las que se hará referencia, asimismo, en las siguientes páginas.

- Un aspecto, en buena medida, clásico dentro de la protección de la esfera privada de la persona es el relativo **derecho a la imagen.** A este respecto, el TEDH ha considerado que la imagen de la persona entra, sin duda, en la esfera de su vida privada, lo que exige que los individuos puedan tener un control sobre dicha imagen. Por ello, en virtud del art. 8 CEDH, los Estados deben proteger al individuo frente a la **captación y difusión de fotografías por parte de los medios de información,** sin consentimiento de los afectados, ya se trate de personajes no públicos o con notoriedad pública, pero realizando actividades de su vida cotidiana o privada (ST. Von Hannover c. Alemania, 24 junio 2004; ST. Sciaccia c. Italia, 11 enero 2005; ST. Reklos y Davourlis c. Grecia, 15 enero 2009). No obstante, lo cierto es que, a lo largo del tiempo, el TEDH ha introducido importantes matizaciones en su jurisprudencia en pro de la libertad de expresión y prensa (Sudre, 2015, p. 692 y 693). En este sentido, la notoriedad pública del afectado, el debate de interés

general suscitado con las informaciones, el contenido y la forma de obtención de las publicaciones o la propia conducta del demandante respecto a la publicidad de su vida privada, juegan en la doctrina del TEDH como factores a valorar y, en su caso, a favor del margen de apreciación a los Estados, no considerándose incumplidas sus obligaciones positivas cuando los tribunales nacionales valoran adecuadamente el conflicto de intereses conforme a tales criterios (ST. Von Hannover c. Alemania, 7 febrero 2012; ST. Alex Springer c. Alemania, 7 febrero 2012). Igualmente proclive a la libertad de prensa se ha mostrado la jurisprudencia de Estrasburgo respecto a las medidas para prevenir y reparar este tipo de injerencias en la vida privada, entendiendo que, pese a que la publicación por un medio en internet de las imágenes grabadas ocultamente de un personaje público realizando prácticas sexuales constituye una flagrante e injustificada invasión de su privacidad, la reparación a través de una indemnización decretada por la justicia nacional resultó adecuada, sin considerar que como parte de las obligaciones positivas de los Estados se debiese cumplir con una medida dirigida a impedir que la imágenes se llegasen publicar, según la costumbre profesional imperante en el Estado de referencia conocida como "pre-notificación" al afectado (ST. Mosley c. Reino Unido, 10 mayo 2011). En cambio, cuando no se trata de un personaje público y la información periodística se considera de escasa relevancia desde el punto de vista del interés general, el TEDH se muestra mucho más favorable a tutelar la imagen de la persona ante la técnica periodística de la cámara oculta (ST. Bremmer c. Turqía, 13 octubre 2015).

En relación con la imagen como aspecto esencial de la vida privada se presentan también los casos relativos a la utilización de la **videovigilancia por parte de las autoridades públicas**. Al respecto, se ha considerado que la simple vigilancia de los comportamientos del individuo en un lugar público no constituye una injerencia en su vida privada, sin perjuicio de que el registro y uso de las imágenes pueda comportar una violación del art. 8 CEDH en relación con la protección de sus datos personales (ST. Peck c. Reino Unido, 28 enero 2003; ST. Perry c. Reino Unido, 17 julio 2003). Así, la filmación secreta de un ciudadano con fines de investigación penal puede constituir una medida legítima siempre que esté debidamente precisada en la legislación nacional, no cumpliéndose estas condiciones cuando la filmación se utiliza como sustitutivo del procedimiento reglado de identificación de sospechosos y sin que ello esté previsto y amparado por la legislación interna (ST. Perry c. Reino Unido. 17 julio 2003). Recientemente, también se ha considerado que no existe una finalidad legítima que justifique la injerencia cuando se instalan cámaras en las aulas de una universidad, espacio considerado por el TEDH un ámbito público donde se desarrolla, sin embargo, la idea de "vida privada social". En tanto que la autoridad universitaria no consiguió demostrar que la instalación y recogida de datos respondía a las finalidades previstas en la legislación sobre protección de datos personales, se consideró vulnerada la vida privada de los profesores que impartían docencia en tales aulas (ST. Antovic y Mirkovic c. Montenegro, 28 noviembre 2017).

Llegados a este punto, cabe hacer referencia, asimismo, a otros diversos pronunciamientos del TEDH relativos al **registro y almacenamiento de imágenes en otras relaciones "inter privatos"**. Así, se ha considerado que la captación de imágenes de un sujeto por parte de una compañía de seguros, sin el consentimiento del primero, para acreditar en fase judicial ciertos comportamientos del mismo que eximirían a la aseguradora de responsabilidad, no constituyó una injerencia ilegítima en la medida que la captación de imágenes con fines judiciales estaba prevista en la ley, perseguía una finalidad legítima y no hubo una difusión de las imágenes más allá de su utilización en el proceso judicial para el fin perseguido (ST. De la Flor Cabrera c. España, 27 mayo 2014). En cambio, en otro caso más reciente de características parecidas, relativo al control por una entidad privada pero actuando con

facultades delegadas de la sanidad pública, se ha considerado que la injerencia no era "conforme a ley" en tanto que la legislación interna no indicaba con suficiente claridad el alcance y la forma de ejercer dicha forma de vigilancia, ni contenía las suficientes garantías frente al abuso en ejercicio de la misma (ST. Vukota-Bojic c. Suiza, 18 octubre 2016).

Los anteriores supuestos guardan, en buena medida, similitud con los supuestos en que un empleador lleva a cabo una videovigilancia de sus trabajadores para detectar hurtos. En un primer caso de estas características, el TEDH consideró que, a pesar de que el Estado no había dispuesto un marco legal que regulase y fijase las condiciones de dicho tipo de vigilancia, los tribunales nacionales habían realizado una ponderación adecuada del conflicto de intereses y la intromisión debía considerarse legítima y proporcionada para proteger el derecho de propiedad empresarial y el interés general en una adecuada administración de la justicia, al no existir ninguna otra medida igualmente eficaz –la observación directa por personas no lo sería– para confirmar las sospechas de hurto (ST. Köpke c. Alemania, 10 octubre 2007). Con todo, ello contrasta con la solución dada en otro supuesto más reciente y muy semejante en que, también ante las sospechas fundadas de hurto, la empresa instaló unas cámaras, algunas de forma visible y otras de forma oculta. En este caso, el TEDH consideró que el Estado había incumplido sus obligaciones positivas al no proteger a las trabajadoras frente a una vigilancia de la que no habían sido informadas suficientemente, actuando, además, la desproporcionadamente al extender el control en el tiempo y a todos los trabajadores; circunstancias que, según el TEDH, diferenciarían a este supuesto del precedente Köpke (ST. López Ribalda y otros c. España, 9 enero 2018 (ver *in extenso infra* III.5). Este asunto está pendiente, sin embargo, de otro pronunciamiento por parte de la Gran Sala del TEDH al haberse aceptado su intervención en virtud del art. 43 CEDH: cuestión grave en relación con la interpretación y aplicación del Convenio.

- El TEDH también ha tenido oportunidad de responder a cuestiones suscitadas en torno a **otras formas de control** sobre la persona, diferentes a aquellas que afectan a su imagen o a sus comunicaciones (véase *infra* II.3.3). Así, desde las perspectiva de las obligaciones negativas del Estado, el TEDH se ha pronunciado sobre la utilización por parte de las autoridades de **sistemas de geolocalización (GPS)**, afirmando que la utilización de estos sistemas de control debe considerarse también una injerencia en la vida privada, si bien la intromisión que comporta es menos grave que otros métodos de control, que captan la imagen o registran las comunicaciones de la persona. Por ello, se consideró que no era necesario que su utilización quedase sujeta exactamente a las mismas garantías previstas para otras injerencias, bastando con que la medida estuviera prevista legalmente, quedase sujeta a control judicial y respondiese proporcionadamente a una finalidad legítima, como se entendió que concurrían en el caso concreto al haberse utilizado este sistema de vigilancia para procesar judicialmente a un sujeto por delitos graves de terrorismo (ST. Uzun c. Alemania, 2 septiembre 2010; ver *in extenso infra* III.2). Ahora bien, si la legislación no es suficientemente precisa sobre en qué condiciones y de qué modo las autoridades están facultadas para utilizar este sistema de control, sí que se produce una injerencia prohibida en la vida privada (ST. Ben Faiza c. Francia, 8 febrero 2018). Así se ha entendido también en un supuesto en que la injerencia consistió en el **acceso por parte de la autoridad a los datos de la dirección IP** en el marco de unas medidas contra la pornografía infantil. La previsión legal utilizada por las autoridades para proceder a tal acceso carecía de claridad, ni preveía el control de las tales facultades por parte de un órgano independiente (ST. Benedik c. Eslovenia, 24 abril 2018).

  El TEDH también ha dado respuesta recientemente a supuestos de **acceso a ficheros electrónicos**. De un lado, ha entendido violado el derecho a la vida privada como consecuencia de la confiscación y acceso por parte de la policía al ordenador depositado,

sin contraseñas ni otras medidas de protección, en un servicio técnico por el presunto autor de delitos de pederastia. Según el TEDH, tal actuación no fue proporcionada al no haberse solicitado la autorización judicial previa normalmente requerida en estos casos, sin que concurriesen en el caso concreto las circunstancias excepcionales –riesgo de eliminación de pruebas o de comisión de nuevos delitos– que, según la legislación nacional, permiten prescindir de tal autorización (ST. Trabajo Rueda c. España, 30 mayo 2017). Por otra parte, el TEDH también ha resuelto el caso de un trabajador de una empresa pública que denunció el acceso a los ficheros de su ordenador, sin su presencia y sin ser informado. La empresa en su reglamento de régimen interior consentía el uso razonable de los medios informáticos para fines privados y la forma en que había guardado el trabajador los archivos en el ordenador permitía intuir o, cuanto menos, sospechar sobre la presencia de elementos de carácter personal. El TEDH juzgó, sin embargo, justificada la injerencia, considerando que las pautas dadas por la jurisprudencia francesa en la materia constituyen la base legal de la injerencia, que la misma perseguía un legítimo –el correcto funcionamiento de la empresa– y que los tribunales nacionales no se habían excedido en su margen de apreciación a la hora de valorar las circunstancias concurrentes de acuerdo con el derecho interno (ST. Libert c. Francia, 22 febrero 2018; ver *in extenso* infra III.6).

Especial referencia a la protección de datos personales

Como se apuntaba en la introducción, en esta materia el Consejo de Europa ha venido desarrollando una importante actividad y ha concretado, en buena medida, el alcance del derecho a la vida privada frente a las amenazas que el desarrollo tecnológico comporta en cuanto al tratamiento de datos personales. El actual **Convenio 108**, tras la reciente reforma operada en 2018, contiene una regulación bastante amplia, cuyos aspectos fundamentales pueden quedar sintetizados del siguiente modo (véase *in extenso* Explanatory Report, cit.):

- El convenio tiene por **objeto** proteger a todas las personas, cualquiera que sea su nacionalidad o residencia, con respecto al tratamiento de sus datos personales (art. 1). Los Estados parte se comprometen a respetar el convenio en su jurisdicción, tanto el sector público como privado, y para ello adoptarán las medidas necesarias en su legislación, las cuales deberán haber entrado en vigor en el momento de la ratificación o adhesión al convenio (arts. 3 y 4). La implementación de los Estados queda expuesta a la evaluación del Comité del convenio, regulado en el mismo, otorgándole, además, otras funciones de tipo interpretativo, consultivo y de proposición de enmiendas al convenio (art. 22 y ss.).
- El convenio recoge las **definiciones esenciales** sobre las que se basa su posterior regulación (art. 2). Así, por "datos personales" se entiende cualquier información relacionada con una persona identificada o identificable; "procesamiento de datos" significa cualquier operación o conjunto de operaciones realizadas con datos personales, tales como la recopilación, almacenamiento, preservación, alteración, recuperación, divulgación, puesta a disposición, borrado o destrucción, o la aplicación de operaciones lógicas y/o aritméticas sobre tales datos. Tras la modernización del convenio por el protocolo de 2018, se aclara que el mismo resulta de aplicación también al procesamiento de datos no enteramente automatizado y, en este sentido, se dispone que cuando no se utiliza un procesamiento automatizado, "procesamiento de datos" significa una operación o conjunto de operaciones realizadas sobre datos personales dentro de un conjunto estructurado de tales datos que son accesibles o recuperables de acuerdo con criterios específicos. Es decir, más allá de los medios y equipos técnicos utilizados, basta la aplicación de criterios predefinidos para individualizar datos para que se aplique el convenio. Por otra parte, "controlador" significa la persona física o jurídica, autoridad pública o sujeto privado, que tenga poder de decisión con respecto al procesamiento de datos. De otro lado, el "destinatario" significa una persona física o jurídica, también pública

o privada, a quien se le revelan o ponen a disposición datos. Finalmente, "procesador" significa una persona física o jurídica, pública o privada, que procesa datos personales en nombre del controlador, abarcando así las situaciones de "delegación" o "subcontratación" en el tratamiento de datos.

- La **legitimidad del procesamiento de datos**, según el convenio, se fundamenta en los siguientes **principios** (art. 5): 1) proporcionalidad de acuerdo con el fin legítimo perseguido; 2) sólo podrán llevarse a cabo tratamientos sobre la base del libre consentimiento, específico, informado e inequívoco del afectado –lo que exige una actividad claramente afirmativa del interesado, sin poder considerar consentimiento válido el derivado del silencio u otras formas de inactividad, como los formularios previamente complementados (Cfr. Explanatory Report, cit., p. 7) o de una base legítima prevista por la ley; 3) los datos deben ser procesados de manera justa y transparente, lo que implica que los fines para los que sean recopilados, además de específicos y legítimos, no sean incompatibles con otros fines legítimos y que su conservación con fines de interés público, investigación científica o histórica o estadística respete las debidas garantías; y 4) el procesamiento debe ser adecuado, relevante y no excesivo en relación con los fines perseguidos, debiéndose actualizar la información cuando sea necesario y conservarse por un tiempo no superior al necesario para los fines perseguidos). La referencia expresa a la proporcionalidad es una novedad de la reciente reforma del convenio que viene a reforzar la previsión relativa al carácter adecuado y no excesivo del tratamiento de datos respecto al fin concreto perseguido, a lo que se le une también como novedad el segundo principio expresado, que viene a reafirmar que sólo caben dos modos de que un tratamiento de datos personales sea legítimo: que cuente con el consentimiento del interesado o que tenga un fundamento previsto por ley.
- En virtud del convenio, hay determinados **datos especialmente sensibles**: los datos genéticos; los relacionados con infracciones y cuestiones penales; los datos biométricos; los datos sobre el origen racial o étnico, opiniones políticas, afiliación sindical, creencias religiosas o de otro tipo, o sobre la salud o vida sexual. Respecto a tales datos, cuyo tratamiento parece comportar un mayor riesgo de violación de los derechos fundamentales, se exige que las legislaciones nacionales adopten garantías adicionales, que protejan especialmente al interesado, particularmente frente al riesgo de discriminación (art. 6). Aspecto destacable tras la reforma de 2018 es la inclusión en este elenco de datos especialmente sensibles de los datos genéticos y biométricos, cuyo tratamiento parece presentar todavía mayores riesgos, por revelar información relativa a la salud y al parentesco, afectando al interesado y a terceros, o por permitir identificar la identidad de una persona de forma única.
- Tanto el "controlador" como el "procesador" deberán, de acuerdo con lo previsto por las legislaciones nacionales, asumir especiales deberes para garantizar la **seguridad de los datos** y evitar el uso no autorizado de los mismos (art. 7). Además, la transparencia en el tratamiento de datos cristaliza en un **deber de información** del controlador al interesado, cuya amplitud es otra las novedades relevantes del protocolo de reforma aprobado en 2018. Este deber de información del controlador va referido a (art. 8): su identidad y residencia o establecimiento habitual, la base legal y los fines del procesamiento de datos, las categorías de datos personales procesados, los destinatarios, en su caso, de los datos, los medios a través de los cuales ejercer los derechos oponibles al tratamiento de datos, así como cualquier información adicional necesaria para garantizar un procesamiento justo y transparente de los datos personales. Si los datos personales no se obtienen del interesado, se podrá excepcionar este deber de información cuando el procesamiento de datos esté previsto expresamente por la ley o cuando el cumplimiento de dicho deber implique

esfuerzos desproporcionados. Más allá de lo expresado literalmente por el convenio, de acuerdo con la finalidad del deber, es obvio que resulta de especial relevancia que la información que se facilite sea fácilmente accesible, legible, comprensible y que se adapte a las características del interesado (Cfr. Explanatory Report, cit., p. 12).

- Los **derechos del interesado** frente al tratamiento de datos son esencialmente los siguientes (art. 9): 1) a no quedar sujeto a una decisión que le afecte significativamente, basada únicamente en un procesamiento automatizado de datos sin tener en cuenta su opinión, salvo que la decisión esté autorizada por ley y ésta contenga garantías adecuadas para tutelar sus derechos; 2) a obtener toda aquella información que el controlador deba proporcionar para garantizar la transparencia del procesamiento de datos de acuerdo con el art. 8 del Convenio; 3) a conocer cuál es razonamiento aplicado al procesamiento de datos; 4) a oponerse en cualquier momento al procesamiento de datos personales, salvo que el controlador acredite fines legítimos que justifiquen el procesamiento; 5) a rectificar y cancelar los datos en procesamiento o procesados en contra de las disposiciones del convenio; 6) a los recursos judiciales y no judiciales apropiados para la tutela de los derechos anteriores, lo que conecta, asimismo, con la obligación de los Estados de establecer sanciones adecuadas en esta materia (art. 12); 7) a la asistencia por parte de las autoridades de supervisión, que todo Estado parte debe disponer para garantizar en su territorio el cumplimiento del Convenio, con facultades informativas, consultivas y sancionadoras (art. 15). A este respecto, de las novedades producto del protocolo de reforma de 2018, cabe destacar la referencia expresa a un derecho a conocer el razonamiento aplicado al tratamiento de datos, lo que constituye un aspecto muy relevante frente a la denominada elaboración de perfiles que, en el actual contexto de profuso uso de los algoritmos, ha adquirido una gran complejidad y sofisticación, hasta el punto que el mero seguimiento del uso de internet permite generar un completo perfil del usuario. Ello, a su vez, está estrechamente conectado con el otro derecho reconocido, también de forma novedosa, a todo interesado a no ser objeto de decisiones significativas sobre la base exclusiva de un tratamiento automatizado de datos –como podría ser la denegación de un préstamo sobre la base de un "*scoring* crediticio" (Cfr. Explanatory Report, cit., p. 13)–, sin tener oportunidad de expresar su punto de vista y poder ejercer otras garantías frente al tratamiento de datos.

- Bajo la alusión a **obligaciones adicionales** (art. 10), el convenio recoge, tras la reforma de 2018, unas disposiciones novedosas cuyo fin es procurar que todo tratamiento de datos minimice los riesgos para la derechos fundamentales de las personas, obligando a que los Estados impongan a los controladores y, en su caso, procesadores de datos, la obligación de prevenir tales riesgos antes de iniciar el procesamiento de datos y diseñen el procesamiento teniendo en cuenta esta prevención, así como a aplicar medidas técnicas y organizativas que tengan en cuenta las implicaciones del derecho a la protección de datos personales en todas las etapas del procesamiento de datos. Con ello, el convenio se está haciendo eco de lo que se conoce como principios de "privacidad desde el diseño" y de "privacidad por defecto" para reducir el impacto de los desarrollos técnicos sobre la protección de datos personales y poner los mismos al servicio de dicha protección. Asimismo, ello compele a adoptar medidas organizativas para asesorar y rendir cuentas en torno al cumplimiento de los derechos en materia de protección de datos, particularmente en las organizaciones complejas, para lo cual puede ser útil la figurada del delegado en materia de protección de datos personales (Cfr. Explanatory Report, cit., p. 15).

- Determinadas disposiciones del convenio y en particular las relativas a los deberes de información del controlador y a los derechos de los interesados pueden quedar sujetas a **excepciones** (art. 11), cuya regulación, tras la reforma operada en 2018, está muy

influenciada por la interpretación que el TEDH ha venido haciendo de las injerencias permitidas en los derechos reconocidos en el CEDH (véase *infra* IV.2). Dispone, en este sentido, el convenio 108 que toda excepción deberá estar prevista por la ley y constituir una medida necesaria y proporcionada en una sociedad democrática con el fin de proteger alguno de los siguientes intereses: la seguridad nacional, la defensa, la seguridad pública, los intereses económicos y financieros importantes del Estado, la imparcialidad e independencia del poder judicial, la prevención, investigación, enjuiciamiento de delitos penales y la ejecución de sanciones penales, así como otros objetivos esenciales de interés público –como puede ser la exigencia de responsabilidad por cualquier otra conducta ilícita, aunque no sea penal–; o, en fin, la protección del interesado o los derechos y libertades fundamentales de los demás, particularmente la libertad de expresión.

Se trata, sin duda, de unas finalidades amplias, si bien, a diferencia de lo que ocurría en la versión original del Convenio (art. 3.2), los Estados ya no cuentan con la posibilidad de hacer declaraciones destinadas a excepcionar la aplicación entera del convenio a ciertos tipos de datos, lo que, en la práctica, permitía excepcionar con carácter más general y sin tener que respetar otras garantías. Además, respecto a las excepciones fundamentadas en razones de seguridad nacional y defensa, precisa el nuevo convenio que las mismas deberán quedar sujetas, de acuerdo con lo previsto en cada legislación nacional, a unos mecanismos de control y supervisión independientes y efectivos, lo que conecta claramente con los pronunciamientos del TEDH relativos a los sistemas de vigilancia masiva de las comunicaciones puestos en marcha por ciertos Estados, en los que el Tribunal ha hecho especial hincapié en que para que los mecanismos de control de las medidas adoptadas por las autoridades sean efectivos, deben encargarse a una autoridad independiente –preferiblemente judicial– y se debe hacer compatible el carácter secreto de la vigilancia con proporcionar algún tipo de información al sujeto para que pueda conocer que sus comunicaciones han sido interceptadas y ejercer, en su caso, los recursos pertinentes (ST. Roman Zakharov c. Rusia, 4 diciembre 2015; ST. Szabó y Vissy c. Hungría, 12 enero 2016). Lo anterior es, asimismo, coherente con lo dispuesto en el Convenio del propio Consejo de Europa en materia de ciberdelincuencia, de 2001 (art. 15).

- Una de las particularidades más significativas del convenio 108 es que se ocupa expresamente de los **flujos transfronterizos de datos personales** (art. 14), dando así respuesta a una de las cuestiones más necesitadas y, a su vez, difíciles de abordar, por el aumento de tales flujos, por el componente de la extraterritorialidad que hace ineficaces las soluciones desde los ordenamientos nacionales y por la necesidad de encontrar un justo equilibrio entre la protección de la privacidad y los importantes intereses económicos presentes detrás de esos flujos (Pavón, 2002, p. 244 y ss.). En este sentido, sin perjuicio de las matizaciones introducidas tras la reforma de 2018, el principio general que consagra el convenio sigue siendo el de libre circulación de datos entre los Estados parte, en tanto que lo mismos garantizan un nivel mínimo de tutela de los datos personales. En estos casos, los Estados no podrán prohibir o condicionar la transferencia de datos a autorizaciones especiales, salvo que ello venga impuesto por normas de protección armonizadas compartidas por los Estados pertenecientes a una organización internacional regional, con lo que claramente se persigue hacer compatible el convenio con el régimen más protector que, en su caso, pueda disponer la Unión Europea.

  Por su parte, cuando el receptor no esté sujeto a la jurisdicción de un Estado parte, la transferencia sólo pueda darse cuando en dicho Estado se garantice un nivel adecuado de protección tomando como referencia las disposiciones del convenio. Dicho nivel de garantías puede venir establecido en leyes de aplicación general –incluidos los acuerdos o tratados internacionales– o en mecanismos jurídicos ad hoc vinculantes para las partes

implicadas en la transferencia y procesamiento de datos –v.gr. cláusulas contractuales que incorporan garantías estandarizadas aprobadas por las autoridades de supervisión en materia de protección de datos o por el propio Comité del convenio (arts. 15.2 y 23)–. Sin embargo, el Convenio 108 también prevé que cada Estado, pese a no existir un nivel adecuado de garantías, permita la transferencia internacional de datos, siempre que se cumpla alguna de las siguientes condiciones: 1) que la misma se produzca con el consentimiento explícito, específico y libre e informado del interesado, entendiéndose el requisito de informado en relación con los riesgos existentes en caso de transferencia a territorios sin garantías adecuadas; 2) o que los intereses específicos del interesado en el caso concreto requieran la transferencia de datos; 3) o que lo requieran otros intereses legítimos, en particular intereses públicos relevantes, siempre que ello esté previsto por ley y constituya una medida necesaria y proporcionada en una sociedad democrática; 4) o que constituya una medida necesaria y proporcionada en una sociedad democrática para la libertad de expresión. Por lo demás, las autoridades de supervisión que deben existir en cado Estado parte deben ser informadas cuando se produzcan transferencias internacionales de datos a Estados no parte o fundamentadas en el propio interés del interesado o de otros intereses públicos, pudiendo tales autoridades prohibir aquellas transferencias no rodeadas de las suficientes garantías o sin acreditación suficiente de intereses legítimos prevalecientes. Estas facultades de la autoridad de supervisión pueden quedar, sin embargo, excepcionadas por razones de seguridad nacional o defensa, siempre que ello se haga por ley y constituya una medida necesaria y proporcionada (art. 11.3).

Hasta aquí una reseña de los principales contenidos sustantivos del convenio 108 que, como ya se apuntó, no genera derechos directamente invocables ante el TEDH, si bien su regulación ha tenido, sin duda, influjo en la jurisprudencia de este Tribunal, guiándose en sus principios para determinar si ha habido o no una injerencia en el derecho a la vida privada (Cfr. Handbook on European data protection law, 2018, p. 25 y ss.). Así, el TEDH viene considerando que la recolección y almacenamiento de toda información relativa a una "persona física identificada o identificable", en el sentido del art. 2 del Convenio 108, interfiere en su vida privada, con independencia de los efectos que ello produzca (ST. Rotaru c. Rumania, 5 de mayo 2000; ST. Amann c. Suiza, 16 febrero 2000; ST. S y Marper c. Reino Unido, 4 diciembre 2008). Y, en este sentido, la **recogida y almacenamiento por parte de las autoridades públicas,** por ejemplo, de imágenes, huellas digitales, archivos de ADN, la ubicación obtenida por GPS o incluso los contenidos de una llamada de teléfono profesional, ha sido considerada una injerencia en la vida privada (ST. Amann c. Suiza, 16 febrero 2000; ST. S y Marper c. Reino Unido, 4 diciembre2008; ST. Uzun c. Alemania, 2 septiembre 2010). Incluso si son datos obtenidos, por ejemplo, por medio de cámaras instaladas en zonas públicas, puede producirse una injerencia en la vida privada como consecuencia del almacenamiento y uso de esas imágenes (ST. Peck c. Reino Unido, 28 enero 2003; ST. Perry c. Reino Unido. 17 julio 2003). Particulares consideraciones ha dedicado el Tribunal a determinados métodos de conservación de datos personales, tales como los ficheros electrónicos de ADN, considerando que dado que permiten descubrir relaciones entre personas constituyen ya de por sí una injerencia en la vida privada, sin que altere la conclusión anterior el hecho de que la información esté codificada y solo pueda revelarse con ayuda de la informática y con conocimientos técnicos (ST. S y Marper. C. Reino Unido, 4 diciembre 2008).

La legitimidad de estas injerencias por parte de las autoridades públicas se hace depender, como en otros ámbitos incluidos en el art. 8 CEDH, de la existencia de un marco legal suficiente, accesible y previsible, que proporcione unas garantías adecuadas dirigidas a asegurar que el tratamiento de datos personales responde a fines legítimos, evitando usos impropios o abusivos. Así, la recogida de datos relativos a los desplazamientos de una persona

en virtud de una orden administrativa no publicada ni accesible de ningún otro modo constituye una clara violación del derecho a la vida privada (ST. Shimovolos c. Rusia, 21 junio 2011). Pero, además, no basta, por ejemplo, con que exista una disposición legal que autorice con carácter general a la conservación de huellas digitales, perfiles de ADN y muestras celulares con fines de prevención y persecución de ilícitos penales, si dicha legislación permite que tal conservación pueda ser indefinida en el tiempo y mantenerse más allá del proceso penal que finalizó sin una condena (ST. S y Marper. C. Reino Unido, 4 diciembre 2008; ver *in extenso* infra III.1. En esta misma línea, ST. Dimitrov-kazarov c. Bulgaria, 10 febrero 2011; ST. M. M. c. Reino Unido, 13 de noviembre2012; ST. M. K. c. Francia, 18 abril 2013; ST. Brunet c. Francia, 18 septiembre 2014). En cambio, se ha considerado una injerencia legítima la prevista en una legislación que ordenaba la inscripción de los responsables de delitos sexuales, en la medida que tal inscripción quedaba limitada en el tiempo, podía quedar sujeta a control judicial y la consulta de los datos registrados estaba reservada a las autoridades competentes, sobre quienes pesaba, además, un deber de confidencialidad (ST. Bouchacourt c. Francia, 17 diciembre 2009). La recogida de datos que responde a una finalidad legítima se convierte, sin embargo, en una injerencia ilegítima cuando los datos son utilizados con una finalidad diferente a la que justificó su recogida (ST. Karabeyoglu c. Turquía, 7 junio 2016). A la luz de estos y otros casos resueltos por el TEDH, se destaca que la protección frente al registro y uso de datos de carácter personal remite a un control especialmente riguroso de la proporcionalidad de la injerencia cometida por las autoridades públicas (Sudre, 2015, p. 695).

Dentro de la protección de los datos personales, el TEDH ha resaltado el carácter especialmente sensible de los **datos relativos a la salud,** en consonancia con lo previsto en el Convenio 108 (ST. S y Marper c. Reino Unido, 4 diciembre 2008). En este sentido, la confidencialidad de los datos médicos se ha considerado un principio esencial y si bien su revelación dentro de un procedimiento administrativo o judicial puede ser una actuación legítima, se produce una violación del derecho en la medida que el Estado no garantice un uso proporcionado de tales datos, permitiendo, por ejemplo, la publicación y difusión de una sentencia en que se hace constar que una persona está afectada por el virus del SIDA (ST. Z. c. Finlandia, 25 febrero 1997, ST. L.L. c. Francia, 10 octubre 2006; ST. C.C. c. España, 6 octubre 2009). La recogida y uso de datos relativos a la salud por parte de las autoridades debe perseguir fines legítimos –como lo sería el control de la calidad de los servicios médicos– y debe ser proporcional a dichos fines. No se cumplen, sin embargo, tales requisitos cuando se constata una recogida indiscriminada y continua de datos y fundamentada en la valoración de la eventual responsabilidad penal de un médico por unos hechos acecidos bastante tiempo atrás y sin que la autoridad en cuestión gozase de competencias para determinar responsabilidades penales (ST. L. H. c. Lituania, 29 abril 2014). Asimismo, desde la perspectiva de las obligaciones positivas, el TEDH ha afirmado la necesidad de que los Estados adopten las medidas dirigidas a garantizar que terceros no hacen un uso no autorizado de datos médicos. En este sentido, se ha considerado que el Estado incumple sus obligaciones cuando no disponen medidas de seguridad apropiadas y permiten que en el ámbito sanitario los empleados pueden acceder a historiales médicos sin dejar rastro (ST. I. c. Finlandia, 17 julio 2008). También se ha condenado al Estado que, en opinión del TEDH, no otorgó una suficiente tutela judicial a un ciudadano frente a la difusión de información médica a la prensa por parte de un servicio sanitario (ST. Biriuk c. Lituania, 25 noviembre 2008).

La jurisprudencia de Estrasburgo también ha sentado, asimismo, criterios acerca del **derecho de los sujetos al acceso a sus datos personales** en posesión de las autoridades públicas. El TEDH en un primer momento se mostró reacio a consagrar un derecho general de acceso a tales datos, sin perjuicio de considerar aquellas situaciones en que concurriese una situación particularmente relacionada con la vida privada, como es el caso del sujeto que habiendo sido

criado bajo la tutela de los servicios sociales solicita información para conocer aspectos de su niñez y de sus años de formación. En tal caso, se consideró que el Estado asume la obligación de permitir al individuo el acceso a la información que le concierna y las limitaciones de acceso deberán estar justificadas en la confidencialidad que pueda afectar a terceras personas (ST. Gaskin c. Reino Unido, 7 julio 1989; no considerando, en cambio, una violación aquella negativa que se fundamenta en proteger la vida privada de terceros, ST. Odièvre c. Francia, 13 febrero 2003). Posteriormente, el TEDH se ha pronunciado con un alcance más amplio, reconociendo, en gran medida, la existencia de un derecho general a acceder a informaciones personales en términos semejantes en los que el art. 8 CEDH protege frente a la recogida, almacenamiento y uso de datos personales; lo que conecta, a su vez, con otros principios esenciales en esta materia, relativos a la posibilidad de controlar el uso que se hace de los datos y poder solicitar su rectificación o destrucción (Lafferty 2014, p. 563 y 564). Así, en varios pronunciamientos, sobre los registros generados por las autoridades de países del este durante las dictaduras comunistas, se deduce la necesidad de que los Estados garanticen a los individuos un procedimiento efectivo para poder acceder a aquella información personal que de forma secreta y que sin precisar sus finalidades específicas puedan conservar las autoridades (ST. Rotaru c. Rumania, 5 de mayo 2000; ST. Turek c. Eslovaquía, 14 febrero 2006; ST. Haralambie c. Rumanía, 27 octubre 2009; ST. Antoneta Tudor c. Rumanía, 24 septiembre 2013)

Finalmente, particularmente reseñable resulta la doctrina sentada por el TEDH respecto a la **cancelación de datos en medios de comunicación digitales** o sobre lo que también se ha dado conocer como **derecho al olvido**. La cuestión ya se planteó, en buena medida, en un caso en que el derecho a la vida privada se invocaba frente a una noticia que cuando fue publicada por un medio de comunicación en la prensa escrita fue objeto de una demanda por difamación admitida por los tribunales y que años después los sujetos afectados por la noticia pretendían que fuera eliminada de la página web del medio en cuestión que la mantenía accesible. Al respecto, el TEDH admitió que internet tiene la potencialidad de almacenar información accesible a millones de usuarios y que por ello representa una amenaza más intensa para el derecho a la vida privada que la prensa tradicional, si bien consideró que la protección de las hemerotecas digitales queda incluida en la libertad de expresión ex art. 10 CEDH, que cubre también el interés legítimo de acceder a archivos digitales de noticias pasadas, como fuente muy valiosa para fines educativos y de investigación histórica, no correspondiendo a las autoridades judiciales reescribir la historia, por lo que son incompatibles con tal libertad medidas que impliquen el borrado o cancelación de tales archivos digitales, sin perjuicio de que sí sean compatibles otras medidas tales como publicar junto con la noticia una advertencia relativa a que la noticia había sido objeto de un pronunciamiento judicial condenatorio (ST. Wegrzynowski y Smolczewski c. Polonia, 16 julio 2013). Muy recientemente, el TEDH se ha vuelto a pronunciar sobre esta temática, en este caso respecto a una demanda que invocaba la violación del derecho a la vida privada como consecuencia de que los tribunales nacionales se habían negado a obligar a varios medios de comunicación digitales a que no se indexaran con nombres personales unas noticias de varios años atrás sobre una condena penal ya cumplida. En este caso, el TEDH reitera criterios ya sentados en la sentencia que se acaba de reseñar y en otros pronunciamientos relativos a la libertad de expresión e información, haciendo prevalecer estas libertades y añadiendo, además, una distinción relevante entre la libertad y funciones asociadas a los editores de la información, que no tienen por qué verse obligados a introducir modificaciones en sus hemerotecas digitales, y los motores de búsqueda en internet, cuya principal función no es proporcionar sino localizar la información, permitiendo en buena medida la elaboración de perfiles de una persona y dando un efecto amplificador a informaciones que pueden interferir en la vida privada (ST. M. L. Y W. W. c. Alemania, 28 junio 2018; véase *in extenso infra* III.7). Por

consiguiente, a la luz de estas sentencias del TEDH, parece que se puede afirmar que el derecho al olvido tiene un diferente alcance frente a los medios de comunicación digitales que frente a los servicios de motor de búsqueda en internet.

II.3.2. Comunicaciones

A pesar de la referencia literal a la "correspondencia" contenida en el art. 8 CEDH, el TEDH no ha dudado en hacer una interpretación actualizada del interés protegido, considerando que toda comunicación privada, cualquiera que sea su forma o el medio utilizado, debe quedar tutelada frente a injerencias arbitrarias (ST. Halford c. Reino Unido, 25 junio 1997; ST. Copland c. Reino Unido, 3 abril 2007). Ante el hecho de que las nuevas tecnologías vienen incrementado las posibilidades de control, el TEDH ha advertido desde hace tiempo que la mera interceptación realizada en secreto aumenta el riesgo de arbitrariedad, debiéndose ser especialmente exigente para justificar tales injerencias (ST. Klass y otros c. Alemania, 6 septiembre 1978). La jurisprudencia del TEDH en este terreno ha tenido oportunidad de pronunciarse también sobre una considerable variedad de situaciones:

- La interceptación de la **correspondencia de las personas privadas de libertad** ha sido considerada en un número relevante de ocasiones una violación del art. 8 CEDH, bien porque la legislación interna no contenía previsiones suficientes sobre este tipo de control o porque el control no respondía a una necesidad debidamente justificada para preservar intereses legítimos (ST. Messina c. Italia, 23 febrero 1993; ST. Rehbock c. Eslovenia, 28 noviembre 2000; ST. Peers c. Grecia, 19 abril 2001; ST. Piskowski c. Polonia, 14 junio 2005). Asimismo, el Estado asume la obligación de garantizar los medios necesarios para que las personas privadas de libertad pueden mantener la correspondencia con el exterior (ST. Cotlet c. Rumanía, 3 junio 2003), lo que no implica, sin embargo, que el no permitir la comunicación por vía electrónica constituya una violación del art. 8 CEDH, siempre que sea posible a través de otros medios (ST. Helander c. Finlandia, 19 diciembre 2013).
- Por otra parte, una copiosa jurisprudencia del TEDH se refiere a **interceptación de las comunicaciones telefónicas por parte de las autoridades públicas.** Tales supuestos son enjuiciados desde la perspectiva más clásica de las obligaciones negativas y constituyen una buena muestra de cómo operan las condiciones previstas en el apartado 2 del art. 8 CEDH a la hora de valorar la legitimidad de una injerencia. A este respecto, la gran mayoría de supuestos se focalizan en la valoración de la concurrencia de la habilitación legal y la necesidad requeridas para justificar la interceptación de las comunicaciones. La doctrina del TEDH viene entendiendo que la legislación que prevea este tipo de controles debe contener garantías adecuadas y efectivas frente a posibles abusos (ST. Klass y otros c. Alemania, 6 septiembre 1978), lo que se concreta en que la legislación debe ser suficientemente clara y precisa, de modo que ofrezca "previsibilidad" respecto al ejercicio de este tipo de control secreto por parte de las autoridades. No se han admitido, en este sentido, las injerencias basadas en regulaciones meramente administrativas, que no precisaban los detalles (ST. Malone c. Reino Unido, 2 agosto 1984), ni tampoco las basadas en una previsión legal de carácter general utilizada por la justicia para ordenar escuchas telefónicas, en la medida que dicha previsión legal no incluía con claridad los fines a los que debe responder y el modo en qué se debe ejercer tal facultad conferida a las autoridades (ST. Kruslin c. Francia, 24 abril1990; ST. Huvig c. Francia, 24 abril 1990; ST. Kopp c. Suiza, 25 marzo 1998; ST. Prado Bugallo c. España, 18 febrero 2003). Estas mismas exigencias legales y la necesidad de respetarlas son predicables respecto a los controles sobre las comunicaciones telefónicas que, aunque no entren a conocer su contenido, afecten a elementos esenciales de las mismas, tales como el destinatario y su duración (ST. Malone c. Reino Unido, 2 agosto 1984; ST. Valenzuela Contreras c. España, 30 julio 1988; ST. Copland c. Reino Unido, 3 abril 2007).

De la jurisprudencia del TEDH se desprende que aspectos tales como qué tipo de personas pueden ser objeto de estas interceptaciones, qué tipo de delitos pueden justificarlas, la duración de las escuchas, el procedimiento para llevarlas a cabo o las condiciones en qué las mismas deben ser destruidas, constituyen aspectos especialmente importantes a considerar por las legislaciones nacionales a la hora de regular la interceptación secreta de las comunicaciones (Lafferty, 2014, p. 556). La previsión de que la interceptación quede sujeta al control de una autoridad independiente también aparece como un elemento relevante para considerar la intromisión como legítima (ST. Koop c. Suiza, 25 marzo 1998; ST. Dumitru Popescu c. Rumania, 26 abril de 2007; ST. Kennedy c. Reino Unido, 18 mayo 2010; ST. Figueiredo Teixeira c. Andorra, 8 noviembre 2016. La autorización *ex ante* de la medida no se considera un elemento absolutamente imprescindible, puesto que un control sustancial *a posteriori* puede compensar la falta de autorización previa (ST. Kennedy c. Reino Unido, 18 mayo 2010), si bien en determinados casos se considera ineludible tal autorización previa, por ejemplo, en relación la vigilancia secreta dirigidas a los medios de comunicación, pues el control posterior no permite salvaguardar un aspecto relevante en la sociedades democráticas como es la confidencialidad de las fuentes periodísticas (ST. Telegraaf Media Nederland Landelijke Media BV y otros c. Holanda, 22 noviembre 2012). El TEDH ha rechazado, en cambio, que entre las garantías que deben acompañar a las interceptaciones se incluya un preaviso al afectado, que pondría en riesgo la finalidad legítima de la medida (ST. Mersch c. Luxemburgo, 10 mayo 1985; ST. Leander c. Suecia, 23 marzo 1987).

Recientemente, el TEDH ha resuelto algunas demandas referidas no tanto a injerencias concretas cuanto a la legitimidad de los sistemas de control de las comunicaciones, a través de las nuevas tecnologías, puestos en marcha por varios Estados en el marco de la prevención del delito y la lucha antiterrorista, que implican la posibilidad de un **control masivo e indiscriminado de las comunicaciones** realizadas a través de la telefonía móvil u otros medios electrónicos. La respuesta del TEDH en estos casos parte introduciendo ciertas matizaciones a la propia doctrina del TEDH, según la cual no es función del Tribunal revisar en abstracto las legislaciones nacionales; matización que, en tales supuestos, tendría que ver con en el propio carácter secreto de la vigilancia, lo que justificaría que, aunque no se pueda probar que se ha producido una injerencia concreta, se pueda recurrir ante el TEDH si se dan las circunstancias para que el sujeto pueda presumir razonablemente ser víctima de una vigilancia secreta sin garantías ni recursos adecuados a la luz de la legislación aplicable (ST. Klass y otros c. Alemania, 6 de septiembre de 1978; ST. Kennedy c. Reino Unido, 18 mayo 2010). Admitido lo anterior, la respuesta dado por el TEDH ha sido rigurosa con la necesidad de que las normativas nacionales que regulen estos nuevos sistemas de control cumplan con las condiciones necesarias para evitar el riesgo de abuso inherente a la vigilancia secreta. El TEDH admite que, como consecuencia natural de las actuales formas de terrorismo, los gobiernos recurran a tecnologías de vanguardia, si bien tales progresos, que permiten recopilar una gran cantidad de datos, se debe acompañar de un desarrollo simultáneo de garantías legales. Y no se produce esta circunstancia cuando la normativa nacional es deficitaria en toda una serie de aspectos clave antes reseñados –circunstancias que justifican la vigilancia; duración de la medida; procedimiento de conservación y destrucción de datos, entre otros–. Además, se hace especial hincapié en que para que los mecanismos de control de las medidas adoptadas por las autoridades sean efectivos, deben encargarse a una autoridad independiente –preferiblemente judicial– y se debe hacer compatible el carácter secreto de la vigilancia –para no frustrar su finalidad– con proporcionar algún tipo de información al sujeto para que pueda conocer que sus comunicaciones han sido interceptadas y ejercer, en su caso, los recursos pertinentes (ST. Roman Zakharov c. Rusia, 4 diciembre 2015; ver *in extenso infra* III.3; ST.

Szabó y Vissy c. Hungría, 12 enero 2016). Otros supuestos pendientes de resolución por el TEDH, como es el caso Big Brother y otros c. Reino Unido (nº 58170/2013) relativo a los programas de vigilancia masiva de las comunicaciones compartidos por los Gobiernos de Reino Unido y Estados Unidos, ofrecerán seguramente más pautas acerca de las condiciones que deben cumplir estos sistemas de control para considerarse legítimos e incluso sobre si los Estados asumen la obligación de proteger a sus ciudadanos frente a las injerencias de otros Estados.

- La protección brindada a las comunicaciones también se ha extendido a la **captación a través de otros medios de conversaciones en espacios privados** ("escuchas" en general), aunque no se produzcan dentro del domicilio, como espacio especialmente protegido por el art. 8 CEDH, sino, por ejemplo, en las dependencias policiales o en una prisión. También en estos casos se exige que la normativa de los Estados precise la posibilidad de llevar a cabo este tipo de injerencias y sus condiciones (ST. Wisse c. Francia, 20 diciembre 2005; ST. Vetter c. Francia, 31 mayo 2005; ST. P.G. y J.H. c. Reino Unido, 25 septiembre 2001; ST. Armstrong c. Reino Unido 16 julio 2002; ST. Bykov c. Rusia, 1 octubre 2009). Y, asimismo, como se apuntaba, semejantes condiciones a las requeridas para justificar la interceptación de las comunicaciones telefónicas han sido exigidas por el TEDH respecto a la **interceptación por parte de las autoridades de comunicaciones electrónicas**, tales como las que se producen a través de los sistemas de "busca", el correo electrónico, así como los datos relativos el uso de internet (ST. Taylor-Sabori c. Reino Unido, 22 octubre 2002; ST. Copland c. Reino Unido, 3 abril 2007; ST. Szabó y Vissy c. Hungría, 12 enero 2016).
- El art. 8 CEDH también se ha considerado aplicable frente a las **injerencias por parte de sujetos privados sobre las comunicaciones electrónicas**. Partiendo de la doctrina ya sentada precedentemente por el TEDH, relativa a las injerencias de autoridades públicas sobre las comunicaciones de sus empleados, que afirmó que las comunicaciones –telefónicas o electrónicas– realizadas desde el lugar de trabajo también pueden quedar incluidas en el ámbito del respeto a la vida privada y de la correspondencia *ex* art. 8 CEDH, existiendo una expectativa razonable de privacidad cuando la recogida y almacenamiento de información relativa a estas comunicaciones se realiza sin el conocimiento del afectado (ST. Halford c. Reino Unido, 25 junio 1997; ST. Copland c. Reino Unido, 3 abril 2007), el Tribunal también se ha pronunciado sobre la interceptación por parte de un empleador privado de las comunicaciones vía internet de sus empleados. En un primer momento, el TEDH consideró que el Estado no había incumplido sus obligaciones positivas, en la medida en que los jueces nacionales habían ponderado adecuadamente el conflicto de intereses, dando relevancia al hecho de que el trabajador había sido informado sobre la prohibición de uso personal de los recursos tecnológicos de la empresa y considerándose razonable el interés del empleador en verificar que los empleados están cumpliendo con sus obligaciones, siendo, además, la injerencia proporcional en tanto que se produjo con el alcance limitado para constatar el incumplimiento laboral (ST. Barbulescu c. Rumanía, 12 enero 2016). Sin embargo, solicitada una revisión del asunto por la Gran Sala del TEDH vía art. 43 CEDH –cuestiones graves de interpretación y aplicación del Convenio–, el nuevo pronunciamiento del TEDH consideró violado el art. 8 CEDH sobre la base fundamentalmente de que para salvaguardar el derecho del trabajador no basta con una indicación general sobre el uso de los recursos electrónicos, sino que es necesaria una indicación previa, clara y precisa sobre la posibilidad de que las comunicaciones sean controladas (ST. Barbulescu c. Rumania, 5 septiembre 2017; ver *in extenso infra* III.4).

III. Algunas sentencias relevantes de la jurisprudencia reciente del TEDH

Teniendo en cuenta que el sistema europeo de derechos humanos es esencialmente un sistema de construcción jurisprudencial y el importante volumen de sentencias emanadas por el TEDH, resulta complejo hacer una selección de la jurisprudencia más relevante referida al derecho a la vida privada. En apartados anteriores, cuando se esbozaba la panorámica general relativa al concepto y alcance de este derecho ya se han citado un buen número de pronunciamientos importantes del TEDH. Por ello, en los siguientes epígrafes se ha optado por hacer una reseña individualizada de algunas sentencias recientes, procurando que en las mismas se aborden diversas cuestiones relevantes para el objeto de estudio. En este sentido, las sentencias seleccionadas se refirieren a cuestiones tales como la protección de datos personales y la inviolabilidad de las comunicaciones frente a las injerencias tanto de poderes públicos como de sujetos privados.

III.1. Registros públicos de huellas, muestras celulares y perfiles genéticos: ST. S. y Marper c. Reino Unido, 4 diciembre 2008

Hechos: Conforme a los hechos declarados, Michael Marper y M.S. –menor de edad–, acusados de violencia de género y robo con violencia, respectivamente y finalmente absueltos solicitaron que se eliminaran de la base de datos policial las huellas dactirales y las muestras de ADN que les habían tomado durante la investigación, a lo que la policía se opuso. Petición que igualmente rechazaron el Tribunal administrativo y el Tribunal de apelación. En la base de tales decisiones está el artículo 64 de la "Police and Criminal Evidence Act" de 1984, que autoriza a conservar las huellas o las muestras de ADN más allá de la fase de investigación, en concreto, para "la prevención y detección de infracciones penales, la investigación de una infracción o el enjuiciamiento posterior".

Agotadas las vías de recurso interno, M. S. y Michael Marper presentaron una demanda ante el TEDH el 16 de agosto de 2004, en la consideración de que la conservación de sus huellas dactilares, muestras celulares y perfiles genéticos en una base de datos policial, una vez que habían sido absueltos de los delitos por los que se les investigaba, resultaba contraria a los artículos 8 y 14 –prohibición de discriminación– del CEDH.

Fundamentación jurídica: Sentado que el registro y conservación de las huellas dactilares, los perfiles de ADN y las muestras celulares suponen una injerencia en el sentido del art. 8 del CEDH, el TEDH analiza si al menos la misma, en el caso analizado, estaba "prevista en la ley", respondía a un fin legítimo y resultaba "necesaria en una sociedad democrática".

En cuanto a la exigencia de **"previsibilidad"** legal, el TEDH conviene con el gobierno británico que el registro y conservación de esos datos personales tenía en el momento de los hechos un fundamento claro en su ordenamiento jurídico. Del mismo modo que quedaba claro en la ley que esos datos se conservarían por tiempo indefinido, salvo supuestos excepcionales. Otra consideración merece, en cambio, para el TEDH la regulación de las condiciones de conservación y uso de esos datos personales, pues desde esa perspectiva el art. 64 resulta mucho menos preciso, pues sólo dispone que las muestras y las huellas no se pueden utilizar para fines distintos de la prevención y detección de infracciones penales, la investigación de una infracción o el enjuiciamiento posterior. Una mención a "la prevención (…) de infracciones penales" que, como declara el TEDH, resulta muy generosa y se presta a una interpretación muy amplia. Máxime porque en este contexto –como en el caso de interceptación de las comunicaciones telefónicas o más ampliamente de vigilancia secreta–, tan importante es

establecer unas reglas claras y precisas sobre el alcance y la aplicación de las medidas como imponer unas condiciones mínimas para la conservación y tratamiento de los datos, respecto de aspectos tales como la duración, la comunicación a terceros, la seguridad y la cancelación de los datos, de manera que los justiciables dispongan de garantías suficientes contra el riesgo de abuso y arbitrariedad.

Desde el punto de vista de si la injerencia litigiosa persigue **"fines legítimos"** y resulta **"necesaria en una sociedad democrática"**, el TEDH no se cuestiona con carácter general el uso de nuevas técnicas de investigación, que ya ha admitido en el pasado, sino si en este caso concreto la conservación de las huellas dactilares y muestras de ADN resultaba proporcionada y reflejaba un equilibrio justo entre el interés público y privado. Algo sobre lo que el Tribunal manifiesta importantes dudas, fundamentalmente por el carácter general e indiscriminado de ese poder de conservación. De un lado, porque, conforme a la ley en vigor en el momento de los hechos, las autoridades podían tomar las huellas dactilares y muestras de ADN de cualquier persona investigada, fuera cual fuera la naturaleza y la gravedad del delito y la edad del sospechoso. De otro lado, porque esos datos se podrían conservar *sine die*, independientemente de la naturaleza o la gravedad del delito investigado o cometido. Además, destaca el Tribunal de Estrasburgo, la probabilidad de que esos registros se cancelaran en algún momento era muy baja, habida cuenta que la ley no contemplaba la existencia de una autoridad externa o independiente que comprobara si tales datos seguían siendo necesarios o pertinentes, en base a criterios concretos, tales como la gravedad del delito, la existencia de antecedentes, el hecho de que persistan las sospechas, etc. Un régimen de conservación indiferenciado e incondicionado que, declara el TEDH, podría comportar un perjuicio importante para los demandantes, habida cuenta del riesgo de estigmatización que supone la conservación de sus datos en esa base policial. Porque, aunque finalmente no se les declaró culpables, a los efectos de la base de datos se les trata como si hubieran sido condenados. Luego tampoco se les considera completamente inocentes. Algo que, añade el TEDH, es aún más grave cuando, como sucede en este caso, afecta a menores de edad. En conclusión, para el TEDH la conservación de la huella dactilar y la muestra de ADN en las condiciones expuestas no asegura el necesario equilibrio entre los interese públicos y privados contrapuestos y excede, por tanto, del margen de apreciación que tienen reconocido los Estados. Se trata de una injerencia desproporcionada y que, por ende, no puede considerarse necesaria en una sociedad democrática, apreciándose por ello una vulneración del art. 8 del Convenio.

III.2. Vigilancia por las autoridades mediante GPS: ST. Uzun c. Alemania, 2 septiembre 2010

Hechos: Conforme a los hechos declarados, las autoridades alemanas ordenaron a principios de los noventa vigilar al Sr. Bernhard Uzun y a su cómplice ante la sospecha de que fueran los responsables de una serie de atentados con bomba. Inicialmente se les sometió a seguimiento por agentes de policía, se instalaron cámaras a la entrada de su domicilio, se interceptó su correo, se intervino el teléfono de sus domicilios y una cabina telefónica cercana, y se instalaron dos emisores en el vehículo con el que se desplazaban. El Sr. Uzun y su cómplice descubrieron, sin embargo, los dispositivos instalados en el vehículo, procediendo a destruirlos. Además, ante la sospecha de que se les estuviera vigilando, dejaron de comunicarse por teléfono y consiguieron en varias ocasiones sustraerse al seguimiento policial. Razón por la cual las autoridades alemanas procedieron a instalar en su vehículo un sistema de geolocalización por satélite –GPS–, que tiempo después permitiría comprobar que el vehículo había estado estacionado a proximidad del lugar donde estalló la siguiente bomba, así como cerca de los lugares en que se fotocopió, escondió y envió las cartas que

reivindicaban el atentado, y del bosque donde los investigadores hallaron los zulos donde habían ocultado el material necesario para la elaboración de los artefactos. Una información que, junto al resto de pruebas –grabación de las cámaras e interceptación de las llamadas– serviría también para acreditar la participación del sr. Uzun en los atentados perpetrados antes de que se les sometiera a una vigilancia mediante GPS, habida cuenta de la similitud de los métodos empleados. A resultas de todo lo cual, el Sr. Uzun fue condenado por el Tribunal de apelación de Düsseldorf a una pena de trece años de prisión por tentativa de asesinato y por cuatro atentados con bomba.

Agotadas las vías de recurso interno, el sr. Uzun presentó el 24 de septiembre de 2005 una demanda ante el TEDH, en la consideración de que la vigilancia mediante GPS y el recurso simultáneo a otras medidas de vigilancia, así como la utilización de los datos resultantes en el marco de un procedimiento penal contra él, habrían comportado una violación de los arts. 8 y 6 –derecho a un proceso justo– del CEDH.

Fundamentación jurídica: El TEDH declara *prima facie* que la vigilancia mediante GPS, así como el tratamiento y la utilización de los datos resultantes, supuso una injerencia en la vida privada del demandante, aun cuando el dispositivo se hubiera instalado en un objeto –un vehículo–, de un tercero –su cómplice– y sólo revelara la ubicación del receptor y no si la persona se encontraba en su interior, pues no en vano, señala el Tribunal de Estrasburgo, la pretensión de las autoridades alemanas era conocer la ubicación y los desplazamientos del demandante y su cómplice.

A continuación, en relación con la "previsibilidad de la ley" y su "compatibilidad con la preeminencia del derecho", el TEDH introduce un matiz importante: su jurisprudencia sobre la interceptación de las comunicaciones no resulta aplicable *mutatis mutandis* al seguimiento de los desplazamientos mediante GPS, en la medida en que la geolocalización supone, en comparación, una injerencia menor en el derecho a la vida privada de las personas. Por consiguiente, los criterios, particularmente restrictivos, que se prevén para el caso de interceptación de las comunicaciones (véase *supra* II.3.2.) no son exigibles en un supuesto como el enjuiciado, aunque, añade, el Tribunal pueda inspirarse en esas garantías mínimas. Ello sin perjuicio de que, añade, la ley tendrá que asegurar en todo caso una protección adecuada y suficiente frente a injerencias arbitrarias o el abuso de poder.

Sentado lo anterior, el Tribunal de Estrasburgo considera que la injerencia en cuestión tuvo una **base legal** clara. En concreto, estima que la expresión "otros medios técnicos especiales destinados a la vigilancia", que figura en el art. 100c § 1.1 b) del Código procesal alemán, da cabida a todos los medios de vigilancia que no sean visuales ni acústicos, que es a lo que se refiere el art. 100c § 1.1 b) del Código procesal alemán. Y considera, por ello, que la aplicación del mencionado precepto por parte de los tribunales alemanes al supuesto enjuiciado constituye una "una evolución razonablemente previsible y una aclaración (…) por vía de interpretación judicial". Por otra parte, el Tribunal de Estrasburgo declara que, en el momento de los hechos, el derecho alemán ofrecía además **garantías suficientes y efectivas frente al abuso de poder**. Desde esta perspectiva, pone en valor el hecho de que, de acuerdo con la ley alemana, los dispositivos de geolocalización sólo pudieran utilizarse para investigar a los sospechosos de delitos muy graves, como fue el caso, y siempre y cuando los otros posibles medios de localización resultaran menos eficaces o fueran difíciles de implementar. El TEDH toma nota de que la ley aplicable no preveía en el momento de los hechos una duración máxima para ese tipo de vigilancia, pero entiende que ello no es incompatible con que tuviera que ser en todo caso proporcionada, algo que, añade, ya comprobaron los tribunales alemanes. Toma nota igualmente de que en el momento en que se produjeron los hechos no se requería autorización judicial para instalar esos dispositivos de geolocalización, pero a pesar

de ello considera que sí existió un cierto control judicial, dado que en el proceso penal posterior el tribunal pudo controlar la legalidad de la medida. Una circunstancia que, unida a la posibilidad de excluir del procedimiento todos aquellos elementos de prueba que se hayan obtenido ilegalmente, constituye, a juicio del TEDH, una garantía importante frente a la arbitrariedad, en tanto que desanima a las autoridades de tratar de obtener pruebas por medios ilegales.

Finalmente, el Tribunal de Estrasburgo considera que la vigilancia en litigio puede considerarse **"necesaria en una sociedad democrática"**, en el sentido del artículo 8.2 del CEDH. Primero, porque se ordenó para investigar varios intentos de asesinato y para prevenir otros posibles atentados con bomba, esto es, en interés de la **seguridad nacional** y de la **seguridad pública**, así como de la protección de los derechos de las víctimas. Y en segundo lugar, porque, vistas las circunstancias del caso, la vigilancia mediante GPS parece una medida **proporcionada**. Desde esta perspectiva, el TEDH destaca el hecho de que no se instalaran los dispositivos GPS desde un principio, sino que las autoridades trataron antes de determinar la participación del demandante en los hechos investigados a través de otros medios menos intrusivos. Ciertamente, como los mismos se revelaron ineficaces, al final el demandante estuvo sometido a múltiples medidas de vigilancia y desde distintas instancias, lo que, reconoce el TEDH, supone una injerencia mayor en el derecho a la vida privada, dado que fueron más los sujetos que tuvieron conocimiento de la actividad del demandante. Ahora bien, como ese seguimiento mediante GPS tuvo lugar durante un periodo de tiempo relativamente corto, únicamente los fines de semana y sólo cuando el sospechoso se desplazaba en el vehículo, a juicio del TEDH el demandante no llegó nunca a estar sometido a una vigilancia total y exhaustiva. Lo cual, unido a la gravedad de los delitos investigados y a la circunstancia de que las medidas de vigilancia que se adoptaron previamente se revelaron insuficientes, lleva al Tribunal de Estrasburgo a concluir que el seguimiento mediante GPS, en los términos descritos, resultó proporcionado y, por tanto, necesario en una sociedad democrática. No apreciándose vulneración del artículo 8 del Convenio.

III.3. Vigilancia secreta y a gran escala por las autoridades públicas: Roman Zakharov c. Rusia, 4 diciembre 2015

Hechos: Conforme a los hechos declarados, el Sr. Roman Zakharov, responsable de una fundación para la defensa de la "Glasnost, interpuso en el año 2003 una demanda contra tres operadoras de telefonía. Alegaba en la misma que se había vulnerado su derecho a la vida privada, porque, en cumplimiento de la Decisión nº 70 de la Comisión Nacional de Comunicaciones y Tecnologías de la Información –predecesor del Ministerio de las Comunicaciones– habían instalado un dispositivo técnico que permitía al Servicio Federal de Seguridad ("la FSB") interceptar cualquier comunicación telefónica sin autorización judicial previa. Motivo por el cual solicitaba a los tribunales rusos que ordenasen la retirada del citado dispositivo y garantizasen que sólo personas debidamente autorizadas podían intervenir las comunicaciones. Pretensión que, sin embargo, no prosperó.

Agotadas las vías de recurso interno, el Sr. Zakharov presentó una demanda ante el TEDH, en la consideración de que el sistema de interceptación de las comunicaciones de telefonía móvil que existía en Rusia vulneraba el artículo 8 del CEDH y porque además no disponía de vías de recurso efectivo contra dicha violación –artículo 13 del CEDH–.

Fundamentación jurídica: Sentado que la vigilancia secreta de las comunicaciones constituye una injerencia en el derecho al respeto de la vida privada y al secreto de la correspondencia, el TEDH se cuestiona si en este caso estuvo suficientemente justificada, en el sentido del artículo 8.2 del CEDH. Más en concreto, como ninguna de las partes discute que

la interceptación de las comunicaciones estaba **prevista en la ley** y que los **objetivos** que se perseguían con dicha vigilancia resultaban **legítimos**, lo que se cuestiona el TEDH es si dicha ley –aunque son varias– cumple con el requisito de **"previsibilidad"** y si la injerencia en cuestión era **"necesaria en una sociedad democrática".**

De acuerdo con lo anterior, el TEDH aborda primero la cuestión de si el derecho ruso define adecuadamente las circunstancias en que las autoridades públicas pueden recurrir a medidas vigilancia secreta como las del caso. Aspecto sobre el que el Tribunal manifiesta importantes dudas. En primer lugar, porque si bien la ley describe de forma precisa los concretos delitos que se pueden investigar mediante la interceptación de las comunicaciones, al mismo tiempo permite tal vigilancia para obtener información de "hechos o actividades que pongan en peligro la seguridad nacional, militar, económica o ecológica" del país. Un supuesto tan amplio y genérico que, considera el TEDH, comporta un riesgo cierto de abuso. En segundo lugar, desde el punto de vista de la **duración de la vigilancia**, el TEDH pone en valor el hecho de que la ley prevea una duración máxima y detalle los casos en que se puede prorrogar la vigilancia, pero, en cambio, echa en falta que no se regulen las circunstancias en que debe cesar la vigilancia cuando la misma se lleva a cabo para salvaguardar la "seguridad nacional, militar, económica o ecológica". Algo que sí se regula cuando dicha interceptación se hace en el marco de una investigación penal. En lo que se refiere a la **conservación, tratamiento, comunicación y destrucción de los datos obtenidos,** el TEDH considera que el derecho ruso fija con carácter general unas reglas claras, que reducen al mínimo el riesgo de acceso o divulgación no autorizada, aunque observa con preocupación que para el caso que los datos hayan servido como prueba en un proceso penal el juez que ha conocido del caso tiene libertad plena para decidir sobre su conservación o destrucción, esto es, sin ningún tipo de condición o límite legal. Por lo que se refiere al **procedimiento de autorización**, el TEDH toma nota de que, como regla general, en el derecho ruso se exige autorización judicial previa, pero también de que ese control judicial es limitado. De un lado, porque la ley no permite al juez examinar aquella información que pueda desvelar la identidad de agentes encubiertos o informantes o datos sobre la organización y la estrategia de la operación de vigilancia, lo que a la postre dificulta comprobar si existe una sospecha fundada sobre la persona a la que se pretende vigilar. De otro, porque la ley ni siquiera impone al juez la obligación de verificar la existencia de tal "sospecha razonable" o de aplicar los criterios de "proporcionalidad" y "necesidad". Observa asimismo el TEDH que las autorizaciones para interceptar comunicaciones en el marco de una investigación penal tienen que identificar de manera precisa a la persona a la que se vigila y el tiempo que durara la medida, y que, en cambio, cuando se trata de investigar hechos o actividades que afectan a la "seguridad nacional, militar, económica o ecológica" la autorización puede referirse más genéricamente a todas las comunicaciones telefónicas de un ámbito geográfico determinado. A lo anterior se añade que, según el derecho ruso, por razones de urgencia se puede prescindir de la autorización judicial. Una posibilidad que el TEDH ha admitido en el pasado, pero siempre y cuando se revistiera de las garantías necesarias para asegurar una utilización prudente y limitada a los casos en que esté debidamente justificado. Lo que, a juicio del Tribunal de Estrasburgo, no sucede en el derecho ruso, toda vez que siempre que esté en peligro grave e inminente la "seguridad nacional, militar, económica o ecológica" las autoridades podrán prescindir de la autorización judicial. Una conclusión que no se desvirtúa por el hecho de que, conforme a la misma ley, un juez tenga que ser inmediatamente informado, pues es sólo a efectos de que autorice, en su caso, la prórroga de esa vigilancia más allá de las cuarenta y ocho horas. El juez no puede entrar a valorar si tal procedimiento de urgencia estaba justificado o decidir si el material grabado a lo largo de esas cuarenta y ochos horas tiene que conservarse o destruirse. Un conjunto de elementos que llevan a concluir al Tribunal de Estrasburgo que los procedimientos de autorización previstos en el derecho ruso no impiden que se someta a los ciudadanos a una

vigilancia secreta arbitraria, irregular o sin un examen motivado. Un riesgo de abuso de poder que se incrementa desde el momento en que, como pone de manifiesto el TEDH, en Rusia el control sobre la implementación de estas medidas de vigilancia secreta no corresponde a los jueces sino que se atribuye a los procuradores. De una parte, porque se suscitan importantes dudas sobre su independencia del poder ejecutivo. Y de otra, porque su capacidad de control es limitada, en cuanto que, como en el caso de la autorización por los jueces, no tienen acceso a aquella información que se refiera a agentes infiltrados de los servicios de seguridad o a los métodos o medios empleados por estos. A lo que se añade que, aunque el procurador puede ordenar que cese la vigilancia, la ley no exige en cambio que se destruya el material ilegalmente obtenido. Una potestad de control por parte de los procuradores que resulta mayormente dudosa en cuanto que no tienen que **rendir cuentas sobre el funcionamiento general del sistema o las concretas medidas adoptadas ante ningún órgano independiente ni ante los ciudadanos**. Una ausencia de garantías adecuadas y suficientes que, a juicio del Tribunal de Estrasburgo, resulta más grave aún desde el momento en que en el derecho ruso no existe una **obligación de informar *a posteriori*** al sujeto cuyas comunicaciones se han interceptado ni una posibilidad real de solicitar y obtener esa información de las autoridades, al igual que tampoco se le ofrece un **recurso administrativo o judicial efectivo** frente a tales interceptaciones. Por todo lo anterior, el TEDH concluye que el conjunto de disposiciones que rige la interceptación de las comunicaciones vulnera el artículo 8 del CEDH, por cuanto no cumplen con las condiciones necesarias para evitar el riesgo de abuso inherente a la vigilancia secreta. Un riesgo que, añade el Tribunal, en este caso es aún mayor, desde el momento en que merced a la Decisión nº 70 los servicios de seguridad y la policía tienen la capacidad técnica de interceptar las comunicaciones sin necesidad de autorización judicial previa.

III.4. Interceptación de la mensajería electrónica de un trabajador por un empleador privado: ST. Barbulescu c. Rumania, 5 septiembre 2017

Hechos: Conforme a los hechos declarados, el Sr. M. Bodgan Mihai Bărbulescu, empleado por una sociedad comercial rumana de derecho privado entre 2004 y 2007, crea, a petición de su empleador una cuenta de *Yahoo Messenger* para comunicarse con los clientes. En dicha empresa el reglamento de régimen interno prohíbe en el momento de los hechos "utilizar los ordenadores, las fotocopiadoras, los teléfonos o los faxes para fines personales", estando acreditado que dicho trabajador fue informado sobre dicho reglamento en el año 2006. Consta asimismo que el 3 de julio de 2007 se distribuyó a todos los empleados una nota informativa, con indicación de que tomaran conocimiento y la firmaran. En dicha nota se recordaba, básicamente, que el tiempo que se pasa en la empresa tiene que dedicarse a trabajar y que no se pueden emplear las líneas de internet, el teléfono o el fax para cuestiones que no afectan al trabajo y se añadía que "el empleador se ve en la obligación de verificar y vigilar el trabajo de los empleados y de tomar medidas de sanción contra las personas que incurran en alguna falta. Vuestras faltas serán cuidadosamente vigiladas y sancionadas!". También se informaba de que una empleada –Sra. B.A.– había sido despedida por razón de las faltas cometidas con respecto a su superior, por el uso que hizo de internet, el teléfono y la fotocopiadora, para fines privados y por su falta de diligencia en el desempeño de sus tareas. En relación con ello, consta que el Sr. Bărbulescu tuvo conocimiento y firmó dicha nota en una fecha indeterminada entre el 3 y el 13 de julio de 2007, así como que el empleador registró en tiempo real las comunicaciones del demandante entre el 5 y el 13 de julio de 2007. Ese día 13 el Sr. Bărbulescu fue informado de que se había vigilado sus comunicaciones a través de *Yahoo Messenger* y que un cierto número de elementos indicaban que había utilizado internet para

fines personales, contraviniendo el reglamento de régimen interno. Se adjuntaron al efecto unos gráficos que indicaban que su volumen de tráfico a través de internet era superior al de sus compañeros de trabajo, pero no se le informó sobre si en el marco de esa vigilancia se había accedido al contenido de sus comunicaciones. Se le requería además para que diera las explicaciones oportunas. Ese mismo día el Sr. Bărbulescu envió un correo en el que negaba tales acusaciones. A la vista de lo cual, el empleador le remitió un nuevo fichero que, esta vez sí, contenía una transcripción literal de las comunicaciones del trabajador con su hermano y su novia, sobre cuestiones personales e incluso íntimas. Finalmente, el 1 de agosto de 2007 el empleador extinguió el contrato de trabajo con el sr. Bărbulescu. Decisión disciplinaria que el trabajador recurrió ante los tribunales, en la consideración de que era ilegal, pero que estos no estimaron.

Agotadas las vías de recurso interno, el sr. Bărbulescu presentó demanda ante el TEDH el 15 de diciembre de 2008, en la consideración de que la decisión de su empleador de extinguir su contrato de trabajo reposaba sobre una previa violación de su derecho a la vida privada y al secreto de la correspondencia –artículo 8 del CEDH– y porque los tribunales nacionales fallaron en su obligación de proteger su derecho.

Fundamentación jurídica: Constatado que los hechos que denuncia el demandante entran de pleno en el ámbito de aplicación del artículo 8 del CEDH, el TEDH aclara antes de nada que este asunto debe examinarse desde la perspectiva de la **obligaciones positivas** (véase *supra* II.2), dado que, aunque la medida contestada la había adoptado una entidad de derecho privado, estaba validada por los tribunales.

Sentado lo anterior, el TEDH declara *prima facie* que los Estados disponen de un amplio margen de apreciación para adaptar su marco normativo a la vigilancia empresarial, habida cuenta de las características específicas del Derecho del Trabajo y de la relación contractual que subyace. Ahora bien, esa libertad, añade, no es absoluta, sino que las autoridades públicas tendrán en todo caso que asegurarse de que la facultad de vigilancia empresarial, que no se discute, vaya acompañada de garantías adecuadas y suficientes frente al abuso. Unos presupuestos de legitimidad de las prácticas empresariales de vigilancia tecnológica que se encarga de concretar el propio Tribunal, a saber: a) **¿El empleado ha sido informado previamente y de forma clara acerca de la posibilidad de que se vigile su correspondencia y las demás comunicaciones, así como de su aplicación efectiva?**; b) **¿Cuál ha sido el alcance de la vigilancia que realiza el empleador y el grado de intrusión en la vida privada del trabajador?** A estos efectos, habrá que distinguir en función de si la vigilancia se limita al flujo de información o alcanza también al contenido, si afecta a la integridad de las comunicaciones o sólo a una parte, si está o no limitada en el tiempo y el número de personas que tienen acceso a los resultados; c) **¿El empleador ha explicitado los motivos legítimos que justifican la vigilancia de las comunicaciones y el acceso a su contenido?**; d) **¿Habría sido posible recurrir a otras medidas o métodos de vigilancia menos intrusivos que el acceso directo al contenido de las comunicaciones del empleado?**; e) **¿Cuáles han sido las consecuencias de la vigilancia para el empleado y de qué manera los resultados se han empleado para alcanzar el objetivo declarado?**; f) **¿Se le han ofrecido al trabajador garantías adecuadas, en particular, frente a las medidas de vigilancia de carácter intrusivo?** Garantías que, añade, deberían impedir que el empleador pueda acceder al contenido de las comunicaciones sin avisar antes al trabajador. A lo que se añade que los trabajadores tienen tener la posibilidad de recurrir ante los tribunales para que estos determinen si, en lo sustancial, se han respetado estas pautas.

Pues bien, partiendo de lo anterior, el TEDH concluye que los tribunales nacionales no tuvieron suficientemente en cuenta los mencionados criterios. Primero, respecto de la exigencia de

transparencia, no se aseguraron de si el trabajador fue informado con carácter previo sobre la naturaleza y el alcance de la vigilancia, entre otras razones porque ni siquiera determinaron en qué momento el empleador accedió al contenido de las comunicaciones en cuestión. En segundo lugar, respecto de la **justificación causal** considera el TEDH que tampoco contrastaron suficientemente la presencia de razones legítimas que justificasen la vigilancia de las comunicaciones. Y en tercer lugar, desde el punto de vista de la **proporcionalidad**, considera igualmente que los tribunales nacionales no examinaron realmente si se podía haber conseguido el mismo fin a través de otros medios menos invasivos para la vida privada y la correspondencia del demandante, algo que, añade el TEDH, resulta mayormente grave porque tampoco valoraron las consecuencias del procedimiento disciplinario que siguió. Un conjunto de consideraciones que, sin perjuicio del margen de apreciación de los Estados, lleva al TEDH a concluir que en este caso las autoridades nacionales no protegieron de manera adecuada el derecho al respeto de la vida privada y de la correspondencia y que, por tanto, se vulneró el artículo 8 del CEDH.

III.5. Videovigilancia de los trabajadores por un empleador privado: López Ribalda c. España, 9 enero 2018.

Hechos: Conforme a los hechos declarados, las Sras. I. López Ribalda, M.A. Gancedo Giménez, M.C. Ramos Busquets, P. Saborido Apresa y C.I. Pozo Barroso, trabajadoras de un supermercado, bajo la fundada sospecha de que se producían hurtos en el establecimiento, fueron sometidas, de forma indiferenciada con el resto de la plantilla, a un sistema de videovigilancia, en concreto mediante unas cámaras visibles y otras ocultas. El objetivo de las primeras era grabar posibles robos por parte de clientes y apuntaban hacia las entradas y salidas del supermercado. El objetivo de las segundas era registrar posibles robos por parte de empleados y por ello apuntaban a los mostradores de salida, que cubrían la zona de detrás de las cajas registradoras. La empresa informo previamente a sus empleados sobre la instalación de las cámaras visibles, pero no en cambio sobre la existencia de cámaras ocultas. Como consecuencia de lo anterior, las mencionadas trabajadoras fueron grabadas robando para sí o en connivencia con clientes. Ante la evidencia de las grabaciones, las cinco trabajadoras reconocieron la falta cometida en presencia de un representante legal de la empresa y un representante sindical y fueron despedidas por razones disciplinarias. Lo anterior no obstante, la empresa llegó antes a un acuerdo con tres de ellas, por virtud del cual una parte reconocía su participación en el robo y se comprometía a no impugnar el despido, y la otra se comprometía a no iniciar acciones penales contra ellas. A pesar de lo cual las cinco trabajadoras ejercitaron finalmente acciones por despido nulo, que, sin embargo, no prosperaron.

Agotadas las vías de recurso interno, las mencionadas trabajadoras presentaron demanda ante el TEDH los días 28 de diciembre de 2012 y 23 de enero de 2013. Alegan que la videovigilancia encubierta ordenada por su empleador, sin informar previamente a las trabajadoras, vulneró su derecho al respeto a la vida privada, así como que los procesos judiciales que siguieron fueron injustos (art. 6 CEDH) desde el momento en que los tribunales declararon la procedencia del despido en virtud de unas grabaciones ilícitas y unos acuerdos firmados bajo presión.

Fundamentación jurídica: Sentado que la captación secreta de la imagen constituye una injerencia particularmente intrusiva en la "vida privada" y que la videovigilancia se realizó por orden del empleador, el TEDH trata de determinar si en este caso concreto el Estado otorgó una tutela adecuada del derecho en litigio frente injerencias de terceros, para lo cual recurre,

aunque de forma algo más confusa, a los tres parámetros de legitimidad jurídica que esboza la ST. Bărbulescu: justificación causal, transparencia y proporcionalidad.

El TEDH destaca, en primer lugar, que la videovigilancia encubierta se llevó a cabo una vez que se constató la existencia de pérdidas y ante la sospecha de que los propios trabajadores o clientes hubieran cometido robos. Sin embargo, a continuación, aprecia que el empleador no informó con carácter previo a los trabajadores. En concreto, destaca que la videovigilancia, que se prolongó a lo largo de un periodo de tiempo prolongado, no cumplió con las exigencias del artículo 5 de la Ley Orgánica de Protección de Datos de Carácter Personal, que establece una obligación de informar previamente, de modo expreso, preciso e inequívoco sobre la existencia de un sistema de registro de datos personales y las características del mismo. Una disposición que, como destaca el TEDH, la propia Agencia Española de Protección de Datos había declarado aplicable a cualquiera que instalara un sistema de videovigilancia. Finalmente, considera el TEDH que el legítimo interés del empleador se podría haber salvaguardado, "al menos hasta cierto punto", "por otros medios, en particular informando previamente a los demandantes, incluso de un modo general, sobre la instalación de la videovigilancia, y proporcionándoles la información descrita en la Ley Orgánica de Protección de Datos de Carácter Personal". Es decir, no sólo **no se habría superado el juicio de transparencia, sino que tampoco se habría superado el juicio de proporcionalidad**, en tanto el empleador tenía, a juicio del TEDH, otros medios menos intrusivos para realizar el control. Un conjunto de consideraciones que llevan al Tribunal de Estrasburgo a concluir que en este caso los tribunales nacionales no fueron capaces de establecer un equilibrio justo entre el derecho de las demandantes al respeto a su vida privada y el interés del empleador en la protección de su derecho a la vida privada, apreciándose, por tanto, una vulneración del art. 8 del CEDH.

III.6. Acceso al ordenador del trabajo de un trabajador por parte de un empleador público: ST. Libert c. Francia, 22 febrero 2018.

Hechos: Conforme a los hechos declarados, el Sr. Eric Libert fue despedido por su empleador tras comprobar que el disco duro de su ordenador de trabajo contenía documentos que habría falsificado en beneficio de terceros y numerosos ficheros de contenido pornográfico. Los archivos en cuestión figuraban en una carpeta denominada "risas" que contenía el disco duro del ordenador del demandante y que a su vez se denominaba "D: datos personales". Denominación que, según se acredita, se da por defecto al disco duro donde los trabajadores guardan los documentos profesionales. Consta asimismo que el empleador tuvo conocimiento previo de la existencia de tales archivos advertido por otro trabajador que accedió al contenido de dicho ordenador mientras el demandante se encontraba suspendido en sus funciones como consecuencia de la apertura de un expediente informativo por denuncia falsa contra un subordinado suyo. Recurrida la extinción del contrato, los tribunales franceses consideraron que existió causa suficiente para despedir al demandante y que no se vulneró su derecho a la vida privada, en tanto que la injerencia no fue desproporcionada.

Agotadas las vías de recurso interno, el Sr. Libert presentó demanda ante el TEDH, en la consideración de que su empleador, al abrir ficheros que figuraban en el disco duro de su ordenador de trabajo, estando él ausente, había vulnerado el artículo 8 del Convenio.

Fundamentación jurídica: Antes de entrar en el fondo del asunto el TEDH deja sentado que estamos ante una injerencia de una autoridad pública, en la medida en que el empleador es un establecimiento público de carácter industrial y comercial, tutelado por el Estado, que además designa a su dirección, y que presta un servicio público. Razón por la cual el asunto debe analizarse desde la perspectiva de las obligaciones negativas y no, como en el caso

Barbulescu, de las obligaciones positivas del Estado. Aclarado lo anterior, el TEDH aborda la cuestión de si tal injerencia estaba "prevista en la ley", la "calidad" de la misma, si perseguía objetivos legítimos y si era "necesaria en una sociedad democrática".

Respecto de la exigencia de **"previsibilidad",** el TEDH considera que existía una base legal para la actuación del empleador y que derecho el francés precisaba suficientemente en qué circunstancias y con qué condiciones se podía realizar tal control. Parte de que los artículos L. 1121-1 y L. 1321-3 del Código de Trabajo tan sólo preveían, de manera muy general, que en el seno de la empresa no se pueden introducir limitaciones a los derechos y libertades individuales y colectivas que no estén justificadas por la naturaleza de las funciones a realizar y que no sean proporcionadas al fin pretendido; pero pone en valor que, en el momento de los hechos, el Tribunal de Casación ya había declarado, por una parte, que los documentos y ficheros creados con el ordenador de trabajo se presumen de trabajo, y, por otra, que el empleador no puede abrir aquellos archivos que el trabajador hubiera identificado como personales. De suerte que, salvo que el trabajador haya identificado un archivo como particular, el empleador puede acceder a todo el contenido del ordenador sin su presencia.

Desde el punto de vista del **"fin legítimo"**, el TEDH rechaza que en este caso pudiera ser "la prevención de infracciones penales", como pretendía el gobierno francés, pero sí admite en cambio como tal la protección de "derechos de un tercero", el empleador, que legítimamente puede aspirar a comprobar que sus trabajadores emplean los medios de producción conforme a las indicaciones dadas por la empresa. En cuanto a la **"necesidad en una sociedad democrática"**, el TEDH destaca que el derecho positivo francés disponía en el momento de los hechos de una garantía adecuada y suficiente frente al abuso: el principio general según el cual el empleador puede abrir los ficheros profesionales del disco duro del ordenador del trabajo de un trabajador, pero, en cambio, no puede acceder subrepticiamente a aquellos otros identificados como "privados", "salvo riesgo o acontecimiento particular". Considera asimismo que los tribunales franceses aplicaron con celo dicho principio al caso, dado que, como constataron, el demandante no había identificado los ficheros como "privados", tal y como específicamente exigía el protocolo remitido por la compañía a los trabajadores, por lo que nada impedía al empleador acceder a los mismos. En consecuencia, concluye las autoridades nacionales no excedieron del margen de apreciación del que disponen y, por tanto, no hubo vulneración del art. 8 del CEDH.

III.7. Derecho al olvido en el ámbito digital: ST. M.L. y W.W. c. Alemania, 28 de junio de 2018

Hechos: Conforme a los hechos declarados, M.L. y W.W., condenados en 1991 a pena de prisión permanente por el asesinato del actor W.S. y que pasaron a situación de libertad condicional en 2007 y 2008, iniciaron en el año 2007 sendos procedimientos judiciales para obtener la supresión de sus nombres de un reportaje titulado "W.S. asesinado hace diez años" que figuraba en la página web de *Deutschalandradio* desde 2010. Sus demandas fueron estimadas por el Tribunal regional de Hamburgo y confirmadas por el Tribunal de apelación de Hamburgo, básicamente porque ambos tribunales consideraron que el objetivo de reinserción debía prevalecer sobre el derecho el derecho de los ciudadanos a ser informados sobre su participación en aquellos hechos. Recurridas en casación, el Tribunal Federal anula, sin embargo, dichas sentencias en la consideración de que las instancias inferiores no habían valorado en sus justos términos la libertad prensa y el interés de los ciudadanos en ser informados.

Agotadas las vías de recurso interno, M.L. y W..W. presentaron demanda ante el TEDH, en la consideración de que la decisión de los tribunales alemanes de no prohibir la puesta a

disposición en internet, por varios medios de comunicación, de reportajes antiguos –o su transcripción– relativos al proceso penal que se siguió contra ellos constituiría una vulneración del art. 8 del CEDH.

Fundamentación jurídica: Sentado que la publicación en los medios de comunicación de informaciones personales constituye una injerencia en la vida privada, el TEDH examina el asunto desde la búsqueda del **equilibrio entre el derecho al respeto de la vida privada del art. 8 del CEDH y la libertad de prensa y el derecho a la información del público**. Partiendo de lo anterior, trae a colación su jurisprudencia sobre el papel de los medios de comunicación en una sociedad democrática, como cuarto poder, y los criterios que ha considerado en el pasado cuando ha tenido que resolver un conflicto entre ambos derechos: el interés general del asunto, la notoriedad de la persona, el objeto del reportaje, el comportamiento previo de la persona afectada, el contenido, la forma y la repercusión de la publicación, así como, en último, término, las circunstancias en que obtuvo la información. Criterios que, considera el TEDH, pueden transponerse al asunto en cuestión, aunque algunos de los mismos puedan ser más o menos pertinentes en función de las circunstancias concurrentes. Porque, señala el TEDH, hay que distinguir entre los medios de comunicación tradicionales y los medios digitales, habida cuenta de la mayor capacidad de difusión y permanencia de estos, lo que sin duda comporta un riesgo mayor para el derecho de respeto a la vida privada, sobre todo como consecuencia de los buscadores. Pues una cosa es la injerencia inicial que resulta de la decisión de un medio de comunicación, incluso digital, de publicar una información y otra la que resulta de los buscadores, que no hacen sino amplificar el alcance de esa injerencia. Un efecto amplificador que, unido a la naturaleza diversa de la actividad que desarrollan, puede hacer que las obligaciones de los buscadores frente a la persona sobre la que se informa sean distintas de las del editor en origen de la noticia. De ahí que los resultados de una eventual demanda de cancelación puedan ser distintos según que se dirija contra el editor inicial de la información, cuya actividad se encuentra en el núcleo mismo de la libertad de expresión, o contra un buscador de internet, cuyo interés principal no es publicar información inicial sobre la persona afectada, sino permitir, de una parte, recopilar toda la información disponible sobre una persona, y, de otra, establecer un perfil de la misma, haciéndose eco, a este respecto, de la jurisprudencia del Tribunal de Justicia de la Unión Europea.

Partiendo de lo anterior, el Tribunal de Estrasburgo aplica al caso cada uno de los criterios citados más arriba. Respecto de la **"contribución al debate general",** la cuestión no se refiere al momento de su publicación, que nadie discute, sino el hecho de que sigan estando disponibles en internet años después, en fechas próximas a la liberación de los demandantes. Es precisamente por ello por lo que concurre un interés legítimo de los demandantes en que se borren esos hechos de su pasado: facilitar su reintegración en la sociedad. Ahora bien, como hacer notar el TEDH, también existe un legítimo interés de los ciudadanos en recibir información no sólo sobre la actualidad sino también sobre acontecimientos del pasado. Ciertamente en este caso las partes no solicitan la supresión de los archivos litigiosos, sino que no figuren sus nombres, lo que por supuesto supondría una restricción menor para la libertad de prensa que la supresión sistemática del reportaje, pero recuerda que el modo en que se elabora una noticia y se define su contenido es parte indisoluble de la libertad de prensa y el art. 10 del CEDH. En concreto, la inclusión del nombre de la persona noticiable constituye un aspecto esencial del trabajo de la prensa y de la credibilidad de la noticia, máxime si se trata como en este caso de un procedimiento penal. Respecto de la **"notoriedad" de los demandantes**, el Tribunal de Estrasburgo concluye que, vista la notoriedad adquirida como consecuencia del crimen y del posterior proceso penal, no puede considerase que fueran personas desconocidas para el gran público en el momento de la presentación de la demanda ante el TEDH. En cuanto al "objeto de los reportajes", parece claro que tanto el proceso penal

como los recursos posteriores son elementos susceptibles de contribuir a un debate en una sociedad democrática. Respecto del **comportamiento de los demandantes** con respecto a la prensa, el TEDH destaca la circunstancia de que ellos mismos filtraron a la prensa numerosa documentación del proceso, así como el hecho de que figurara en la página web de uno de los abogados defensores numerosos reportajes sobre su cliente. En cuanto al "**contenido, forma y repercusión de la publicación"**, ninguna duda hay sobre la veracidad y objetividad de los reportajes, mientras que el grado de difusión, que es lo que se cuestiona por los demandantes, es a juicio del TEDH limitado, vista su ubicación en la página web, pues no llamaría la atención de aquellos internautas que no buscaran específicamente información sobre los demandantes. Ciertamente, como señalan estos, gracias a los buscadores de internet se produce un efecto amplificador, dado que permite, independientemente del grado de difusión inicial, encontrar información sobre ellos de manera permanente, pero llegado a este punto, advierte el TEDH, no consta que los demandantes se hubieran dirigido previamente a las empresas que explotan los buscadores para reducir las posibilidades de que se encuentren esas informaciones sobre sus personas, además de que el Tribunal no puede pronunciarse sobre la posibilidad de ordenar la adopción de otro tipo de medidas que supongan una restricción menor a la libertad de expresión si no fueron objeto de debate previo en la jurisdicción nacional. Un conjunto de consideraciones que llevan a Tribunal de Estrasburgo a concluir que, visto el margen de apreciación de las autoridades nacionales, la importancia de mantener a disposición reportajes sobre cuya veracidad y objetividad nadie discute y el comportamiento de los demandantes con respecto a la prensa, el estado alemán no habría faltado a su obligación de proteger su derecho a la vida privada.

IV. La naturaleza del derecho al respeto de la vida privada

IV.1. Un derecho humano limitado

El derecho a la vida privada *ex* art. 8 CEDH, en tanto que integrado en un convenio internacional que tiene como fuente de inspiración la Declaración Universal de Derechos Humanos y en consonancia con el propio Preámbulo del Convenio, debe ser considerado un derecho predicable de todo sujeto en los regímenes verdaderamente democráticos (Casadevall, 2012, p. 34 y 35). En la práctica, ello comporta, tal y como se colige de los arts. 1 y 13 del CEDH, la aplicabilidad directa de los derechos consagrados en el CEDH a todo individuo sujeto a la jurisdicción de un Estado parte del convenio –sin limitaciones por su nacionalidad, edad o cualquier otra circunstancia personal–, siendo éste el titular del derecho y pudiendo invocarlo directamente ante las jurisdicciones internas y posteriormente ante el TEDH (Renucci, 2015, p. 26 y 27). Es más, a pesar de su naturaleza de derecho inherente a la persona, a la luz de algunos pronunciamientos del TEDH, no cabe descartar que también haya intereses de las personas jurídicas merecedores de tutela en virtud del art. 8 del CEDH (Cfr. Handbook, cit., p. 84), por ejemplo, cuando la injerencia, además de afectar a una persona física, puede redundar en perjuicio de la imagen y credibilidad de una sociedad mercantil (ST. Niemietz c. Alemania, 16 diciembre 1992; ST. Bernh Larsen Holding AS y otros c. Noruega, 14 marzo 2013). Y desde la perspectiva de los sujetos activos de la injerencia, la doctrina del TEDH relativa a las obligaciones positivas dimanantes para los Estados permite afirmar, como se vio, que el derecho a la vida privada reconocido en el CEDH tiene una doble eficacia: vertical –frente a las injerencias de los poderes públicos– y horizontal –frente a las injerencias de otros sujetos privados–.

De la jurisprudencia del TEDH no se deducen, asimismo, límites al derecho a la vida privada conectados al ámbito económico o social en que se pretende ejercer el derecho, más allá de los que se derivan indirectamente de la propia delimitación –como se ha visto, generalmente muy amplia– de lo que se considera vida privada y de la delimitación –menos amplia– de las injerencias que cabe considerar legítimas en virtud del propio CEDH. En este sentido, el apartado 2 del art. 8 CEDH no deja dudas, como ya se apuntó, de que el derecho a la vida privada reconocido en el Convenio no es un derecho absoluto, pues el citado artículo se encarga de precisar las condiciones que pueden justificar una injerencia por parte de las autoridades. Se encuentra, de este modo, el derecho reconocido en el art. 8 CEDH entre los llamados derechos restringidos o condicionados del Convenio (Casadevall, 2012, p. 36 y 169). Tales límites responden a un visión pragmática y realista de los redactores del TEDH y las construcciones jurídicas en torno a los mismos se han convertido, a la postre, en una parte fundamental e indisociable de la garantía de los derechos inherentes a toda persona humana (Renucci, 2015, p. 84). En el siguiente epígrafe se ofrece una perspectiva general de cómo el TEDH viene interpretando tales condiciones que justifican una injerencia, así como otras limitaciones que pueden adoptar los Estados en determinadas circunstancias excepcionales.

Tales condiciones *ex* art. 8.2 CEDH están previstas en relación con las injerencias permitidas a las autoridades y, por tanto, juegan a priori tan sólo con respecto a las obligaciones negativas y no como límites a las obligaciones positivas para los Estados. En este último caso, como se apuntaba anteriormente, el enfoque adoptado por el TEDH descansa en una valoración más libre sobre el justo equilibrio entre los intereses del individuo y el interés general (Lafferty, 2014, p. 524 y 532 y ss.), si bien en dicha valoración pueden adquirir a menudo cierta relevancia los condiciones y fines del apartado 2 del art. 8, lo que conecta con la idea expresada a menudo por el TEDH de que los principios aplicables a las obligaciones positivas y negativas del Estado son en buena media comparables o similares (entre otras, ST. Keegan c. Irlanda, 26 mayo 1994;

ST. Dickson c. Reino Unido, 4 diciembre 2007; ST. Barbulescu c. Rumania, 5 septiembre 2017). En este sentido, como se expondrá a continuación, algunos elementos incardinables en "la protección de los derechos y las libertades de los demás" parecen adquirir especial transcendencia a la hora de determinar los límites a las obligaciones positivas de los Estados en torno al derecho de la vida privada.

IV.2.Las injerencias legítimas (arts. 8.2 y 15 CEDH)

De acuerdo con el enfoque clásico de resolución de las demandas por violación del art. 8 CEDH, el TEDH examina, en primer lugar, la aplicabilidad del Convenio al concreto supuesto de hecho, determinando la existencia o no de una injerencia en el ámbito de protección del citado artículo. Y una vez afirmada la aplicabilidad del Convenio, la segunda fase consiste en analizar si la injerencia constatada puede considerarse justificada desde el punto de vista de lo recogido en el apartado 2 del art. 8. Dado que tales exigencias son, en buena medida, comunes a los derechos garantizados en los arts. 8 a 11 CEDH, no debe extrañar que la doctrina sentada respecto a otros derechos haya sido traslada al derecho reconocido en el art. 8 (por ejemplo: ST. Silver y otros c. Reino Unido, 25 febrero 1983; ST. Matwiejczuk c. Polonia, 2 diciembre 2003). Resulta, en este sentido, posible esbozar una descripción general del test utilizado por el TEDH a la hora de enjuiciar la legitimidad de las injerencias, sin perjuicio de las modulaciones o matizaciones que tal test puede sufrir respecto a cada materia o caso concreto, tal y como se ha podido apreciar en cierta medida cuando se han reseñado las algunas de las manifestaciones del derecho a la vida privada (véase *supra* II.3). Del apartado 2 del art. 8 CEDH se coligen tres requisitos para que una injerencia pueda entenderse legítima:

- La primera exigencia es que la injerencia esté **prevista por la ley**. Dicho de otro modo, las injerencias deben tener fundamento jurídico en el derecho nacional y ello debe ser entendido en sentido material y no formal, lo que tiene varias consecuencias. De un lado, la "ley" en el sentido del apartado 2 del art. 8 CEDH incluye también el derecho no escrito, particularmente la posible doctrina de los tribunales supremos y/o constitucionales establecida al interpretar y completar las disposiciones escritas, sin que haya motivo para dar menos relevancia a la jurisprudencia en los países de tradición continental que en los del *common law* (ST. Kruslin c. Francia, 24 abril 1990, ST. Huvig c. Francia; Sentencia de 24 de abril de 1990). La doctrina de los Tribunales ha sido, en efecto, considerada importante a la hora de valorar la legitimidad de la injerencia en determinados casos relativos, por ejemplo, a la interceptación de las comunicaciones u otros registros sobre elementos propios de la esfera privada de la persona (ST. Koop c. Suiza, 25 marzo 1998; ST. Valenzuela Contreras c. España, 30 julio 1998, ST. Stés Colas Est y otros c. Francia, 16 abril 2002; ST. Libert c. Francia, 22 febrero 2018). Si no resulta posible hallar una base legal, en el sentido expresado, que regule la injerencia, la misma no puede ser considerada "conforme a la ley" y constituye una violación del derecho a la vida privada, sin necesidad de examinar sin concurren el resto extremos requeridos para justificar una injerencia (ST. Copland c. Reino Unido, 3 abril 2007).

  Por otra parte, que el requisito de "previsto por la ley" no se circunscriba a aspectos formales tiene como consecuencia que el fundamento jurídico de las injerencias debe valorarse desde la perspectiva de lo que TEDH denomina como "calidad de la ley". El propio derecho que permite la injerencia debe ofrecer unas ciertas garantías contra las injerencias arbitrarias de las autoridades, otorgándole así un carácter protector a la "preeminencia del derecho" que pone en valor el Preámbulo del CEDH (ST. Malone c. Reino Unido, 2 agosto 1984). Entre las exigencias integrantes de la "calidad de la ley" están la accesibilidad y la previsibilidad. Por un lado, la ley debe ser suficientemente accesible: el ciudadano debe disponer de información suficiente, en las circunstancias del caso, sobre las normas

jurídicas aplicables. Por otro lado, una norma sólo puede ser considerada como "ley" si está formulada con la precisión suficiente para permitir al ciudadano regular su conducta y prever en un grado razonable las consecuencias que una acción determinada puede acarrear (ST. Sunday Times c. Reino Unido, 26 abril 1979; ST. Malone c. Reino Unido, 2 agosto 1984; ST. Leander c. Suecia, 23 marzo 1987; ST. Costello-Roberts c. Reino Unido, 25 marzo 1993). Ahora bien, el TEDH es consciente de que es poco realista pensar que la ley pueda regular de forma exhaustiva todos los límites de un derecho, no oponiéndose a la idea de previsibilidad el hecho de que la ley reconozca un poder discrecional, siempre que la norma precise con suficiente claridad la finalidad y alcance de tal poder, de manera que el ciudadano pueda intuir que se está ejerciendo arbitrariamente y pueda reaccionar a través de procedimientos adecuados para la tutela de sus derechos (ST. Malone c. Reino Unido, 2 agosto 1984). Particularmente, en materia de protección de datos personales y cuando se trata de medidas de vigilancia secreta, el TEDH suele ser especialmente exigente a la hora de valorar cuando una ley reúne las garantías adecuadas (Casadevall, 2012, p. 171).

- En segundo lugar, la injerencia prevista por el Derecho nacional debe obedecer a uno de los **fines legítimos** previstos en el apartado 2 del art. 8: "la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás". En páginas precedentes ya se pudo ver como alguna de estas finalidades aparecen habitualmente consignadas en las injerencias permitidas por el TEDH. Conviene destacar ahora que el bienestar económico del país es la única finalidad que aparece como justificativa de las limitaciones al derecho a la vida privada que no aparece en las restricciones permitidas a otros derechos recogidos en el Convenio. Esta finalidad, más allá de su conexión con la posibilidad de recopilar datos a efectos de la prevención de delitos económicos (ST. Funke c. Francia, 27 enero 1993), puede ponerse en relación con la recogida en el Convenio 108 en materia de protección de datos que, tras la reciente reforma de 2018, alude a "importantes intereses económicos y financieros del Estado" (art. 11.1a), lo que incluiría, en particular, el tratamiento de datos dirigido a facilitar la recaudación de impuestos y el control de divisas (Cfr. Explanatory Report, cit., p. 16). En este sentido, el TEDH ha admitido como legítima una transferencia de datos bancarios entre autoridades de dos Estados amparada en el cumplimiento de un acuerdo internacional sobre asistencia mutua en materia tributaria (ST. G. S. B. c. Suiza, 22 diciembre 2015).

  Por lo demás, no es infrecuente que el TEDH afirme las finalidades previstas en el art. 8.2 deben ser interpretadas de forma restrictiva en tanto que excepciones a un derecho, por lo que se exige que su concurrencia en cada caso concreto se justifique de forma convincente (ST. Klass c. Alemania, 6 septiembre 1978; ST. Rotaru c. Rumania, 4 mayo 2000, ST. Stés Colas Est y otros c. Francia, 16 abril 2002). No obstante, los cierto es que en la mayoría de casos el cumplimiento de la finalidad legítima no supone un serio obstáculo ante el TEDH (Casadevall, 2012, p. 171). Así, en el caso de interceptación de las comunicaciones o de utilización de datos personales, aunque no concurra el consentimiento del afectado, ante la alegación más habitual de las autoridades de fines relativos a la seguridad nacional, la defensa del orden o la prevención del delito, el TEDH entiende cumplido el requisito, resaltando el amplio margen de apreciación de los Estados (ST. Klass y otros c. Alemania, 6 septiembre 1978; ST. Leander c. Suecia, 23 marzo 1987; Z. c. Finlandia, 25 febrero 1997).

- En tercer lugar, la injerencia no sólo debe obedecer a una de las anteriores finalidades, sino que además debe ser **"necesaria en una sociedad democrática".** Sobre esta locución, el TEDH ha apuntado algunos criterios de delimitación, considerando que "necesario" no equivale a la exigencia más rigurosa de "indispensable", si bien la noción no tiene la flexibilidad de otras expresiones, tales "admisible", "útil", "razonable" o "deseable" (ST.

Silver y otros c. Reino Unido, 25 febrero 1983) La traducción jurídica de la expresión "necesidad social imperiosa" utilizada habitualmente por el TEDH no ha sido otra que la aplicación del principio de proporcionalidad, como máxima no escrita, a la hora de valorar la legitimidad de la injerencia en los derechos reconocidos en el CEDH, operando a modo de límite de los límites a tales derechos (Fassbender, 1998, p. 52 y ss.). El TEDH lleva a cabo generalmente una diferenciación del principio en dos momentos: en primer término, determina la necesidad de la medida y, en segundo lugar, tiene en cuenta la proporcionalidad en sentido estricto de la medida, ponderando los medios empleados y los fines perseguidos. Para el TEDH una medida es necesaria cuando existe un motivo justo, pertinente y suficiente que lleve al Estado a limitar un derecho. Sin motivos suficientes la medida no será necesaria y, por tanto, no estará justificada. En todo caso, los Estados disponen de un cierto margen de apreciación a la hora de valorar la necesidad, dada su proximidad y contacto directo con las fuerzas vivas del país (ST. Handyside c. Reino Unido, 7 diciembre 1976; ST. Silver y otros c. Reino Unido, 25 febrero 1983; ST. Buckey c. Reino Unido, 25 septiembre 1996).

Este tercer requisito se ha revelado crítico dentro del sistema del Convenio, tanto desde una perspectiva cuantitativa, pues en un elevado número de casos la principal discusión se centra en el examen de esta cuestión, como cualitativa, en tanto que los principales problemas que suscita la jurisprudencia del TEDH estriban en la dificultad de objetivar las ponderaciones entre fines y medios que realiza el Tribunal para valorar la proporcionalidad de la medida, sin obviar al mismo tiempo el "margen estatal de apreciación", cuya consideración por el TEDH responde a la necesidad de no cuestionar demasiado las decisiones de las autoridades nacionales que actúan bajo principios de responsabilidad democrática y de respetar la diversidad política y cultural de la Europa democrática. Cuanto menor consenso aprecia el TEDH respecto a una materia, menos riguroso es el mismo a la hora de ponderar el principio de proporcionalidad frente al margen de apreciación estatal (Fassbender, 1998, p. 55 y ss.). Resulta, por ello, enormemente difícil establecer pautas generales respecto al modo en que el TEDH viene aplicando este requisito, pudiéndose, a lo sumo, establecer criterios por grupos de casos o materias (Grabenwarter, 2014, p. 207).

En otro orden de consideraciones, dentro de las injerencias permitidas, hay que hacer alusión a lo previsto en el art. 15 CEDH que, de forma similar a lo recogido en otros convenios internacionales en materia de derechos fundamentales, contempla la posibilidad de una **derogación temporal de las obligaciones de los Estados** derivadas de ciertos artículos del CEDH, entre ellos el art. 8, en determinadas situaciones excepcionales. De acuerdo, en efecto, con el artículo 15 CEDH, en los supuestos de **"guerra" u "otro peligro público que amenace la vida de la nación"**, los Estados parte podrán tomar medidas que deroguen el ejercicio de algunos derechos garantizados por el mismo, pero "en la estricta medida en que la situación lo exija", lo que, a su vez, debe ponerse en relación con los arts. 17 y 18 CEDH, que prohíben el abuso de derecho en la interpretación de cualquier disposición del convenio y en particular de las limitativas de derechos (Casadevall, 2012, p. 174 y 176). Salvo error u omisión, no hay constancia de ningún pronunciamiento del TEDH que se haya tenido que pronunciar sobre esta derogación en relación con los derechos reconocidos en el art. 8 CEDH. En todo caso, de la jurisprudencia del TEDH relativa a otros derechos –especialmente en casos de derogación del derecho de libertad *ex* art. 5 CEDH y habiendo el Estado alegado amenazas de terrorismo–, se desprende que para concurra el presupuesto habilitante es necesaria una situación de riesgo excepcional e inminente, que suponga una amenaza para la vida organizada de la comunidad que representa el Estado, si bien puede bastar con que el peligro afecte solo a una parte del territorio (ST. Lawless c. Irlanda, 1 julio 1961; ST. Irlanda c. Reino Unido, 18 enero 1978). Asimismo, el TEDH ha hecho particular hincapié en la justa proporcionalidad entre la

medida adoptada y la amenaza, así como en la imposibilidad de que la aplicación de la medida implique discriminaciones entre nacionales y extranjeros prohibidas por el propio CEDH (ST. Branningan y McBride c. Reino Unido, 26 mayo 1993; ST. Demir c. Turquía, 23 septiembre 1998; ST. A. y otros c. Reino Unido, 19 febrero 2009). Desde el punto de vista formal, la adopción de estas medidas de derogación exigen que el Estado mantenga al Consejo de Europa plenamente informado sobre sus fines y alcance (art. 15.3 CEDH). Ante las graves amenazas de terrorismo que vienen constatándose en las últimas décadas, la opinión que parece predominante en el seno del propio Consejo Europa es que el art. 15 CEDH se configura como un mecanismo adecuado y suficientemente adaptable para combatir tales amenazas, exhortando a los Estados miembros a limitar este tipo de medidas a aquellas medidas necesarias, razonables y proporcionados (Renucci, 2015, p. 24 y 25).

IV.3. La tutela de los derechos de los demás como límite a las obligaciones positivas

Como se apuntó, a menudo resulta difícil apreciar diferencias significativas en el enfoque adoptado por el TEDH a la hora de valorar una injerencia desde la perspectiva de las obligaciones negativas o positivas de los Estados. Respecto a estas últimas, el TEDH suele recurrir al uso de cláusulas de estilo, que aluden a la justa ponderación entre el interés general y los intereses del individuo y, por ello, se ha afirmado que resulta bastante complejo extraer de la doctrina del TEDH unas pautas metodológicas claras acerca del alcance de las obligaciones positivas y sobre los intereses que se están ponderando en cada caso concreto, objetándose la falta de una mayor argumentación (Lafferty, 2014, p. 590 y 591). Con todo, de algunos supuestos resueltos por el TEDH cabe deducir como el citado interés general se concreta con mayor precisión en la defensa de determinados derechos de terceros, que actúan como límites al derecho a la vida privada.

- De un lado, la protección de la **vida privada de otros sujetos**, conectada a su vez con un deber de confidencialidad de las autoridades, aparece en ocasiones como límite a las obligaciones positivas del estado en torno al respeto de la vida privada del reclamante ante el TEDH. Así se desprende de aquellas cuestiones planteadas ante el TEDH en que la vulneración del art. 8 CEDH se vincula con la imposibilidad de obtener datos que le permitan al sujeto conocer sus orígenes (ST. Gaskin c. Reino Unido, 7 julio 1989; ST. Mikulic c. Croacia, 7 febrero 2002; ST. Odièvre c. Francia, 13 febrero 2003). Ahora bien, en estos casos las autoridades no pueden oponer sin más un derecho a la vida privada frente a otro, sino que asumen ciertas obligaciones procedimentales, en el sentido de que la ponderación de intereses en conflicto se lleve a cabo a través de un procedimiento con garantías adecuadas y con intervención de un órgano independiente (ST. Gaskin c. Reino Unido, 7 julio 1989). Por lo demás, en otros casos las legislaciones y prácticas nacionales deberán ser especialmente cuidadosas a la hora de valorar que manifestación de la vida privada debe primar, so pena de incumplir con sus obligaciones positivas; lo que se entiende que se produce cuando se da prioridad a la confidencialidad en el uso de internet frente a la persecución de delitos que afectan a la privacidad e integridad de un menor (ST. K. U. c. Finlandia, 2 diciembre 2008).
- Por otra parte, como límite a la vida privada y a las obligaciones positivas de los Estados aparece significativamente la **libertad de expresión**, que es otro de los derechos consagrados por el CEDH (art. 10) y que comprende la libertad de opinión y de recibir o comunicar informaciones o ideas, sin que pueda haber injerencia de autoridades públicas, salvo cuando se cumplan condiciones muy similares a los que se exigen para poder limitar el derecho a la vida privada. En esta materia, la jurisprudencia del TEDH revela una clara

inclinación en favor de tales libertades frente a diversas manifestaciones del derecho a la vida privada. El interés general de las opiniones, informaciones u imágenes, muchas veces ligado a la relevancia o notoriedad pública del sujeto al que se refieren, ha sido el elemento fundamentalmente utilizado por el TEDH para considerar justificadas determinadas injerencias en la vida privada en el ámbito periodístico o publicatario (ST. Polanco Torres y Movilla Polanco c. España, 21 septiembre 2010; ST. Mater c. Turquía, 16 julio 2013; ST. Von Hannover c. Alemania, 7 febrero 2012; ST. Alex Springer c. Alemania, 7 febrero 2012; ST. Bohlen c. Alemania; 19 febrero 2015; ST. Fürst-Pfeifer c. Austria, 17 mayo 2016). Y seguramente esta tendencia del Tribunal es la que ha llevado a que en un ámbito tan relevante, en el actual contexto, para la tutela de vida privada como es la protección de datos personales, la cláusula contenida en la versión original del Convenio 108, que permite a los Estados apartarse de los principios de la protección de datos para proteger los derechos de los demás, haya venido leyéndose principalmente en clave de protección de la libertad de expresión y así ha quedado reflejado en la reciente reforma del citado convenio, que ahora cuando se refiere a "los derechos y libertades fundamentales de los demás" añade "particularmente la libertad de expresión" (art. 11.1b). Como se vio, la libertad de expresión introduce importantes limitaciones en el alcance de un derecho, especialmente significativo en la era digital, como es derecho a cancelación o modificación de datos o también denominado derecho al olvido (ST. M. L. Y W. W. c. Alemania, 28 junio 2018). Asimismo, la libertad de expresión aparece expresamente mencionada como elemento que puede justificar excepciones a las disposiciones sobre flujos transfronterizos de datos personales, dando prioridad a la libre circulación de datos en favor de dicha libertad de expresión frente a otros intereses (art. 14.4 d). Con todo, por amplio que quepa interpretar el elemento relativo al interés general, el mismo se desvanece si no hay una proporcionalidad en el sacrificio de un derecho –protección de datos– frente al otro –libertad de expresión e información–, tal y como ocurre cunando empresas privadas ofrecen servicios que permiten conocer datos fiscales de más de 1,2 millones de personas (ST. Satakunnan Markkinapörssi Oy and Satamedia Oy c. Finlandia, 29 junio 2017).

- Otro elemento que, a la luz de la doctrina del TEDH, se puede destacar como fin que justifica limitaciones en las obligaciones positivas del Estado relativas al respeto de la vida privada es la defensa de los **intereses económicos de terceros.** Ello, a su vez, puede quedar a menudo conectado con un interés particular y también general a una adecuada administración de justicia –nótese que la imparcialidad e independencia judicial aparecen, asimismo, como fines legítimos que justifican excepciones a los principios y derechos en materia de protección de datos personales, de acuerdo con el Convenio 108 (art. 11.1 a)–. Es cierto que, en comparación con lo que se acaba de señalar en relación a las limitaciones que la libertad de expresión puede suponer para el derecho a la vida privada, esta otra limitación no aparece reflejada de una forma tan vigorosa en la jurisprudencia del TEDH, aunque queda patente en determinados de supuestos como en el que se rechaza que se produzca una violación del derecho como consecuencia de que una compañía de seguros tome imágenes de un sujeto, sin su conocimiento, para defender en juicio su interés a no ser responsable de una indemnización económica (ST. De la Flor Cabrera c. España, 27 mayo 2014), así como en otros supuestos en que se han enjuiciado diversas formas de control empresarial sobre los empleados –v.gr. videovigilancia; interceptación de las comunicaciones– y en los que el TEDH ha aludido al derecho de propiedad empresarial o al interés empresarial al buen funcionamiento de la organización y, por tanto, a verificar que los trabajadores están cumpliendo debidamente sus obligaciones, como fines legítimos que pueden justificar una injerencia en la vida privada (ST. Köpke c. Alemania, 10 octubre 2007; ST. Barbulescu c. Rumania, 5 septiembre 2017; ST. López Ribalda y otros c. España, 9 enero 2018). Cuestión diversa es que también en este tipo de conflictos el TEDH

viene exigiendo, en buena medida, el cumplimiento del resto de condiciones derivadas del apartado 2 del art. 8 –fundamento legal, calidad de la ley y carácter proporcional de la medida–.

V. Conclusiones

Desde una perspectiva general, considerando el carácter amplio y expansivo que el TEDH viene otorgando a la noción de respeto a la vida privada consagrada en el art. 8 CEDH, con fundamento en la concepción de "instrumento vivo" que se le atribuye al Convenio, cabe afirmar que en el sistema europeo de derechos humanos este es un derecho suficientemente protegido y que, además, este sistema dispone de mimbres idóneos para ir dando respuesta a los desafíos se presentan en el actual "mundo digital". Tal afirmación se ve, en buena medida, confirmada teniendo en cuenta que el Consejo de Europa viene mostrando desde hace más de 40 años una particular preocupación por las amenazas que las nuevas tecnologías comportan para la privacidad, habiendo integrado en el contenido del derecho a la vida privada la protección de los datos personales a través del Convenio 108, cuya muy reciente modernización ha obedecido precisamente a la constatación de una nueva morfología e intensificación de los procesamientos de datos personales y los flujos de los mismos. Obviamente, más allá de la importancia del acceso de los ciudadanos a la protección jurisdiccional del TEDH, la efectividad combinada de estos instrumentos internacionales dependerá, en gran medida, de que los Estados implementen en los ordenamientos nacionales un nivel de garantías adecuado.

La conclusión general anterior se mantiene a pesar de que el derecho a la vida privada no se configura en el sistema del Consejo de Europa como un derecho absoluto y que sobre el papel las injerencias permitidas por el art. 8.2 CEDH aparecen como muy amplias. Sin embargo, a la luz de la interpretación exigente que el TEDH viene haciendo de las condiciones que se deben dar para considerar legítimas tales injerencias, es posible afirmar también desde una perspectiva general que tales excepciones constituyen una parte fundamental e indisociable de la garantía de los derechos fundamentales, actuando como estándar mínimo de protección en los Estados pertenecientes al Consejo de Europa (Freixes, 1995, p. 101 y ss.). La impronta de tales construcciones garantistas del TEDH también se deja sentir claramente en la regulación de las excepciones permitidas por el Convenio 108 en materia de protección de datos personales.

Con todo, no hay duda de que, incluso desde la perspectiva protectora que ofrece el sistema de europeo de derechos humanos, la digitalización sigue enfrentando al derecho a la vida privada a importantes desafíos. Como se apuntó, frente al elemento de la extraterritorialidad que caracteriza al actual escenario tecnológico es prioritario promover una armonización internacional de la protección del derecho a la vida privada. De nada sirve reconocer derechos frente a la digitalización a nivel nacional si no resultan aplicables a sujetos que se encuentran allende de las fronteras. Las innovaciones tecnológicas y de comunicación de los siglos XIX y XX comportaron la creación de organismos internacionales destinados a facilitar cooperación entre los países y un cuerpo de normas comunes, pero eso no ha sucedido en el caso de internet. Ciertamente, la normativa de protección de datos tanto de la UE y, a los efectos que aquí más interesan, del Consejo Europa, ambas reformadas en tiempos recientes, constituyen importantes pasos en ese sentido. La legislación europea vincula incluso a sujetos no establecidos en la UE, pero que ofrezcan o proyecten bienes o servicios en el ámbito de la UE o tengan acceso a información de usuarios –como cookies– radicados en territorio europeo. Una dimensión supranacional de la protección de datos de carácter personal a la que puede contribuir significativamente el Consejo de Europa. La versión original del convenio no solo ha sido ratificada por la práctica totalidad de los países europeos, sino que también lo han ratificado Estados que no forman parte del Consejo de Europa, como Uruguay o Cabo Verde. Habrá que esperar a ver si el reciente protocolo de modificación del Convenio, que incluye novedades importantes para hacer frente a los retos de la digitalización, tiene el mismo grado

de adhesión entre los Estados. Particularmente relevante, en el sentido de hacer frente al desafío de la extraterritorialidad, resulta la regulación recogida en el Convenio 108 en cuanto a la transferencia internacional de datos personales, en la medida que el principio general que consagra es que la libertad de circulación de datos está permitida siempre que en el Estado de destino de los datos, sea o no parte del convenio, exista un nivel adecuado de protección de los datos personales tomando como referencia las disposiciones del convenio; lo que, sin duda, puede contribuir a que tanto los Estados como los operadores estén interesados en una armonización de las legislaciones nacionales en este sentido, apostando por una liberalización de los datos con garantías y beneficiosa para todos.

Por otra parte, conocida la capacidad tecnológica que ahora tienen los Estados para realizar actividades de vigilancia secreta, masiva y preventiva, si quieren aprovechar de forma adecuada tales ventajas que ofrece el desarrollo tecnológico no deberían dudar en evaluar y, en su caso, revisar sus marcos jurídicos en materia de interceptación de las comunicaciones para asegurar su adecuación a los principios en materia de derechos humanos y, en particular, al derecho a la vida privada. En este sentido, si, como decíamos, las injerencias permitidas por el CEDH y su interpretación por el TEDH constituyen una garantía inescindible del derecho fundamental, también se presentan al mismo tiempo como una garantía de la preservación de los intereses generales, tales como los que están implicados en la defensa de la seguridad nacional, en particular en la lucha contra el terrorismo u otras formas de crimen organizado. Aunque sensibles a los horrores de la primera mitad del siglo XX, los padres fundadores eran conscientes de que las sociedades democráticas corren un alto riesgo si los derechos de ciertos sujetos no se sacrifican en beneficio de la mayoría. Tal y como ya reconoció en 1978 el TEDH, en una sociedad democrática es necesario un cierto grado de vigilancia de las comunicaciones para proteger la seguridad (ST. Klass y otros c. Alemania). Ahora bien, una cosa son unas escuchas en el marco de una investigación policial o judicial y otra bien distinta es registrar toda la actividad telefónica o de internet con carácter preventivo. En este sentido, hay un consenso bastante generalizado entre los Estados y las organizaciones internacionales en considerar desproporcionadas las medidas de vigilancia masiva e indiscriminada (Cfr. la Resolución 68/167 de la Asamblea General de las Naciones Unidas sobre "El derecho a la privacidad en la era digital". Y también el conocido como "Informe Moraes" del Parlamento Europeo, nº 2013/2188(INI)). Y ello es lo que, en gran medida y en su calidad de receptor y difundidor de los consensos entre los Estados democráticos, recoge la doctrina del TEDH. Parece, por tanto, llegado el momento de comprobar si los marcos legales, los procedimientos y prácticas de vigilancia se ajustan a doctrina del TEDH, pues sólo en la medida en que las legislaciones nacionales se adapten a dicha doctrina las autoridades de las mismas podrán aprovechar de forma adecuada y proporcionada el potencial de las nuevas formas y metodologías de vigilancia sin recibir el reproche de la comunidad internacional.

Al hilo de lo anterior, los Estados no sólo tienen que abstenerse en su vigilancia de injerencias arbitrarias o desproporcionadas, sino que, dado el componente de la extraterritorialidad, se plantea la importante cuestión de asegurar, además, la protección de la vida privada de sus nacionales frente a las injerencias de terceros Estados. No parece que hasta la fecha se haya dictado por el TEDH ningún pronunciamiento que aborde claramente esta cuestión, pero parece fuera de toda duda que el art. 8 del CEDH obliga a los Estados a adoptar esa posición vigilante y cumplir con sus obligaciones positivas también frente a otros Estados (Cfr. Salamanca, 2014, p. 21 y ss.). En este sentido, la pauta establecida por el Convenio 108 es, sin duda, indicativa, ya no sólo por exigir garantías en el flujo internacional de datos personales, obligando ello a evaluar la legislación y las garantías del país de destino, sino también porque cualquier excepción a las principios en materia de protección de datos basada en la seguridad nacional necesita cumplir con los mismos parámetros exigidos por el TEDH para las injerencias

permitidas en los derechos humanos; esto es, que ello esté previsto por ley y constituya una medida necesaria y proporcionada en una sociedad democrática. Por consiguiente, del nivel de adhesión y seguimiento de las pautas fijadas por el Convenio 108 dependerá también, en buena medida, que se pueda avanzar frente al desafío de la extraterritorialidad en punto a la vigilancia por parte de las autoridades públicas.

En otro orden de consideraciones, la protección suficientemente amplia que cabe predicar del derecho a la vida privada en el sistema del Consejo de Europa también se pone de manifiesto si se repara en que, a pesar de su original formulación en términos clásicos de relaciones Estado-ciudadano, tal derecho y su protección a través del TEDH, gracias a su doctrina relativa a las obligaciones positivas, despliega un efecto horizontal; esto es, tutela frente a las injerencias de otros sujetos particulares o en otro tipo de relaciones privadas. Asimismo, el Consejo de Europa fue pionero en sentar principios relativos a la protección de datos personales en el sector privado y el ámbito de aplicación del Convenio 108 no sólo se extiende a los ámbitos públicos y privados, sino que gran parte de sus contenidos están claramente orientados a preservar esta esfera de la privacidad frente a ciertas prácticas de las actividades comerciales.

Con todo, a la luz de los casos a los que ha tenido que ir enfrentándose el TEDH, llama la atención que los conflictos derivados de eventuales injerencias en el derecho a la vida privada cometidas por sujetos privados se estén focalizando cuantitativamente en dos parcelas: el ámbito de las posibles injerencias cometidas por los medios de comunicación y el ámbito de las posibles injerencias sobre la vida privada de un trabajador en el marco de una relación de trabajo por cuenta ajena. En cambio, salvo error u omisión, cabe afirmar que la jurisprudencia del TEDH está prácticamente huérfana de supuestos en que este tipo de conflicto de intereses se haya planteado en otros ámbitos u otras relaciones jurídicas en que aparentemente puede ser también habitual, máxime en el actual contexto de absoluto protagonismo de internet en la vida cotidiana de las personas, y que guardarían relación con lo que en términos generales podríamos llamar protección de datos personales de los consumidores. Habría que analizar si esta situación también es propia de los conflictos suscitados ante las autoridades y jurisdicciones nacionales y cuáles pueden ser las razones que la explican, que se antojan múltiples y muy variadas. A los efectos que aquí interesan, cabría, en todo caso, apuntar una posible causa de este escenario que tendría que ver con lo apuntado en la introducción de este estudio en cuanto a la necesidad de avanzar en la "garantía" del "efecto útil" de la protección de los datos personales, en el sentido de que puede ser insuficiente con el reconocimiento general de unos derechos en esta materia, si ello no va acompañado de otros mecanismos que permitan a los sujetos ser realmente conscientes de sus derechos y del modo de ejercerlos. Ciertamente, en esta línea parecen moverse varias de las novedades introducidas en la reciente reforma operada sobre el Convenio 108, tales como el ampliado deber de información del controlador del procesamiento de datos personales al sujeto afectado por el mismo, que se extiende incluso a la información que permita conocer el razonamiento aplicado al tratamiento de datos y que en ocasiones puede quedar estrechamente conectado con el derecho reconocido, también de forma novedosa, relativo a no ser objeto de decisiones significativas sobre la base exclusiva de un tratamiento automatizado de datos sin tener oportunidad de expresar su punto de vista y poder ejercer, en su caso, otras garantías frente al tratamiento de datos. De la capacidad de los Estados de trasponer y garantizar el cumplimiento de estas garantías en sus ordenamientos nacionales, junto con una tarea de información y sensibilización en la materia, dependerá, en buena medida, la efectividad del derecho a la privacidad del consumidor en la actual era digital, sin perjuicio de reconocer que se trata de una tarea no fácil, dada la multitud de sujetos intervinientes en este contexto, y de que en este terreno también es conveniente un actitud

prudente y equilibrada que evite el riesgo de una suerte de "psicosis" por los datos personales que puede acarrear más disfunciones –sobre todo de tipo económico– que beneficios.

Por último, respecto a esos dos ámbitos en que se vienen focalizando los casos resueltos por el TEDH, destaca el vigor con que la jurisprudencia del TEDH –y también el Convenio 108– subraya la libertad de expresión como límite al derecho a la vida privada, confrontando los dos derechos y apuntado una serie de criterios –interés general de la información, notoriedad pública y propia conducta del afectado– que, a la postre, vienen a conceder a los Estados un amplio margen de apreciación en favor de la libertad de expresión. En cambio, respecto a las intromisiones en la vida privada en el ámbito laboral, la jurisprudencia el TEDH es mucho menos explícita y categórica a la hora de señalar los intereses que se contraponen a la vida privada, que en la mayoría de casos podrían quedar claramente conectados con el derecho a la propiedad reconocido en el art. 1 del Protocolo nº1 al CEDH. Probablemente, esta menor determinación a hora de poner manifiesto los derechos enfrentados lleve a que no siempre se le de relevancia a un que elemento que parece que podría ser determinante para enjuiciar estos asuntos con principios equilibrados, cual es considerar la propia conducta de quien invoca el derecho a la vida privada, por ejemplo, incumpliendo las reglas fijadas en la empresa sobre el uso no personal de los recursos electrónicos o realizando comportamientos todavía más graves, como hurtos. Por lo demás, los criterios manejados y las conclusiones sentadas en estos casos relativos al ámbito laboral, sin perjuicio de las particularidades del caso concreto, parecen a veces poco uniformes, dando la sensación que el TEDH no es siempre igual de riguroso a la hora de valorar la legitimidad de la injerencia desde la perspectiva del resto de condiciones exigidas de acuerdo con el art. 8.2 CEDH: injerencia prevista y con garantías en la ley y proporcionalidad de la misma. Ello no deja de producir ciertas paradojas y disfunciones desde el punto de vista de la virtualidad de la jurisprudencia del TEDH como estándar mínimo de protección de los derechos recogidos en el convenio, no proporcionando a los Estados, en comparación con otras materias, pautas suficientemente claras sobre cómo abordar esta cuestión en sus ordenamientos nacionales.

Lista de sentencias del TEDH citadas

1. ST. Lawless c. Irlanda, 1 julio 1961
2. ST. Handyside c. Reino Unido, 7 diciembre 1976
3. ST. Irlanda c. Reino Unido, 18 enero 1978
4. ST. Klass y otros c. Alemania, 6 septiembre 1978
5. ST. Sunday Times c. Reino Unido, 26 abril 1979
6. ST. Marckx c. Bélgica, 13 junio 1979
7. ST. Dudgeon c. Reino Unido, 22 octubre 1981
8. ST. Silver y otros c. Reino Unido, 25 febrero de 1983
9. ST. Durini c. Italia, 12 enero 1984
10. ST. Malone c. Reino Unido, 2 agosto 1984
11. ST. X e Y contra Países Bajos, 26 marzo 1985
12. ST. Mersch c. Luxemburgo, 10 mayo 1985
13. ST. Rees c. Reino Unido, 17 octubre 1986
14. ST. Jhonston y otros c. Irlanda, 18 diciembre 1986
15. ST. Leander c. Suecia, 23 marzo 1987
16. ST. Valenzuela Contreras c. España, 30 julio 1988
17. ST. Gaskin c. Reino Unido, 7 julio 1989
18. ST. Kruslin c. Francia, 24 abril 1990
19. ST. Huvig c. Francia, 24 abril 1990
20. ST. Niemietz c. Alemania, 16 diciembre 1992
21. ST. Funke c. Francia, 27 enero 1993
22. ST. Messina c. Italia, 23 febrero 1993
23. ST. Costello-Roberts c. Reino Unido, 25 marzo 1993
24. ST. Branningan y McBride c. Reino Unido, 26 mayo 1993
25. ST. Keegan c. Irlanda, 26 mayo 1994
26. ST. Kroon y otros c. Países Bajos, 27 octubre 1994
27. ST. Buckey c. Reino Unido, 25 septiembre 1996
28. ST. Z. c. Finlandia, 25 febrero 1997
29. ST. Halford c. Reino Unido, 25 junio 1997
30. ST. M. S. c. Suecia, 27 agosto 1997
31. ST. Kopp c. Suiza, 25 marzo 1998
32. ST. Sheffield y Horsham c. Reino Unido, 30 julio 1998
33. ST. Demir c. Turquía, 23 septiembre 1998

34. ST. Lustig-Prean y Beckett c. Reino Unido, 27 septiembre 1999
35. ST. Amann c. Suiza, 16 febrero 2000
36. ST. Rotaru c. Rumania, 5 mayo 2000
37. ST. Mikulic c. Croacia, 7 febrero 2002
38. ST. Rehbock c. Eslovenia, 28 noviembre 2000
39. ST. Peers c. Grecia, 19 abril 2001
40. ST. P.G. y J.H. c. Reino Unido, 25 septiembre 2001
41. ST. Stés Colas Est y otros c. Francia, 16 abril 2002
42. ST. Pretty c. Reino Unido, 25 abril 2002
43. ST. Goodwin c. Reino Unido, 11 julio de 2002
44. ST. Armstrong c. Reino Unido 16 julio 2002
45. ST. Taylor-Sabori c. Reino Unido, 22 octubre 2002
46. ST. Peck c. Reino Unido, 28 enero 2003
47. ST. Odièvre c. Francia, 13 febrero 2003
48. ST. Prado Bugallo c. España, 18 febrero 2003
49. ST. Cotlet c. Rumanía, 3 junio 2003
50. ST. Perry c. Reino Unido, 17 julio 2003
51. ST. Y. F. c. Turquía, 22 julio 2003
52. ST. Matwiejczuk c. Polonia, 2 de diciembre de 2003
53. ST. M.C. c. Bulgaria, 4 diciembre 2003
54. ST. Glass c. Reino Unido, 9 marzo 2004
55. ST. Von Hannover c. Alemania, 24 junio 2004
56. ST. Chauvy y otros c. Francia, 29 junio 2004
57. ST. Sciaccia c. Italia, 11 enero 2005
58. ST. Novoseletskiy c. Ucrania, 22 febrero 2005
59. ST. Vetter c. Francia, 31 mayo 2005
60. ST. Piskowski c. Polonia, 14 junio 2005
61. ST. Roche c. Reino Unido, 19 octubre 2005
62. ST. Wisse c. Francia, 20 diciembre 2005
63. ST. Turek c. Eslovaquía, 14 febrero 2006
64. ST. Grant c. Reino Unido, 23 mayo 2006
65. ST. Trocellier c. Francia, 5 octubre 2006
66. ST. L.L. c. Francia, 10 octubre 2006
67. ST. Jaggi c. Suiza, 13 julio 2006
68. ST. Copland c. Reino Unido, 3 abril 2007

69. ST. Dumitru Popescu c. Rumania, 26 abril de 2007
70. ST. I. c. Reino Unido, 11 julio 2007
71. ST. Köpke c. Alemania, 10 octubre 2007
72. ST. Pfeifer c. Austria, 15 noviembre 2007
73. ST. Dickson c. Reino Unido, 4 diciembre 2007
74. ST. McGinley y Egan c. Reino Unido, 9 junio de 2008
75. ST. Biriuk c. Lituania, 25 noviembre 2008
76. ST. K.U. c. Finlandia, 2 diciembre 2008
77. ST. S y Marper c. Reino Unido, 4 diciembre 2008
78. ST. Reklos y Davourlis c. Grecia, 15 enero 2009
79. ST. A. y otros c. Reino Unido, 19 febrero 2009
80. ST. A. c. Noruega, 9 abril 2009
81. ST. Codarcea c. Rumanía, 2 junio 2009
82. ST. Bykov c. Rusia, 1 octubre 2009
83. ST. C.C. c. España, 6 octubre 2009
84. ST. Haralambie c. Rumanía, 27 octubre 2009
85. ST. Bouchacourt c. Francia, 17 diciembre 2009
86. ST. Kennedy c. Reino Unido, 18 mayo 2010
87. ST. Uzun c. Alemania, 2 septiembre 2010
88. ST. Polanco Torres y Movilla Polanco c. España, 21 septiembre 2010
89. ST. Dimitrov-kazarov c. Bulgaria, 10 febrero 2011
90. ST. Mosley c. Reino Unido, 10 mayo 2011
91. ST. Shimovolos c. Rusia, 21 junio 2011
92. ST. M. C. c. Rumanía, 27 septiembre 2011
93. ST. Von Hannover c. Alemania, 7 febrero 2012
94. ST. Alex Springer c. Alemania, 7 febrero 2012
95. ST. Wilson c. Reino Unido, 23 octubre 2012
96. ST. Telegraaf Media Nederland Landelijke Media BV y otros c. Holanda, 22 noviembre 2012
97. ST. M. K. c. Francia, 18 abril 2013
98. ST. Mater c. Turquía, 16 julio 2013
99. ST. Wegrzynowski y Smolczewski c. Polonia, 16 julio 2013
100. ST. Antoneta Tudor c. Rumanía, 24 septiembre 2013
101. ST. Delfi AS c. Estonia, 10 octubre 2013
102. ST. Söderman c. Suecia, 12 noviembre de 2013

103. ST. Vilnes y otros c. Noruega, 5 de diciembre de 2013
104. ST. Helander c. Finlandia, 19 diciembre 2013
105. ST. L. H. c. Lituania, 29 abril 2014
106. ST. De la Flor Cabrera c. España, 27 mayo 2014
107. ST. Brunet c. Francia, 18 septiembre 2014
108. ST. Bremmer c. Turquía, 13 octubre 2015
109. ST. Roman Zakharov c. Rusia, 4 diciembre 2015
110. ST. G. S. B. c. Suiza, 22 diciembre 2015.
111. ST. Szabó y Vissy c. Hungría, 12 enero 2016
112. ST. Barbulescu c. Rumanía, 12 enero 2016
113. ST. Fürst-Pfeifer c. Austria, 17 mayo 2016
114. ST. Karabeyoglu c. Turquía, 7 junio 2016
115. ST. Vukota-Bojic c. Suiza, 18 octubre 2016
116. ST. Figueiredo Teixeira c. Andorra, 8 noviembre 2016
117. ST. Trabajo Rueda c. España, 30 mayo 2017
118. ST. Satakunnan Markkinapörssi Oy and Satamedia Oy c. Finlandia, 29 junio 2017
119. ST. Barbulescu c. Rumania, 5 septiembre 2017
120. ST. Antovic y Mirkovic c. Montenegro, 28 noviembre 2017
121. ST. López Ribalda y otros c. España, 9 enero 2018
122. ST. Ben Faiza c. Francia, 8 febrero 2018
123. ST. Libert c. Francia, 22 febrero 2018
124. ST. Benedik c. Eslovenia, 24 abril 2018
125. ST. M. L. Y W. W. c. Alemania, 28 junio 2018.

Bibliografía

ANDREJEVIC, M.: Spy: Surveillance and Power in the Interactive Era, Ed. University Press of Kansas, 2007.

ARZOZ, X.: "Derecho al respeto de la vida privada y familiar", Convenio Europeo de Derechos Humanos**,** BIB 2009\5398 (http://www.aranzadidigital.es).

CASADEVALL, J.: El Convenio Europeo de Derechos Humanos, el Tribunal de Estrasburgo y su jurisprudencia, Ed. Tirant lo Blanch, Valencia, 2012.

COUNCIL OF EUROPE: Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series, No. 223, 2018 (https://rm.coe.int/16808ac91a).

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS/COUNCIL OF EUROPE.: Handbook on European data protection law, Luxemburgo, 2018.

FASSBENDER, B.: "El principio de proporcionalidad en la jurisprudencia del Tribunal Europeo de Derechos Humanos", Cuadernos de derecho público, nº 5, 1998.

FREIXES, T.: "Las principales construcciones jurisprudenciales del Tribunal Europeo de Derecho Humanos: El standard mínimo exigible a los sistemas internos de derechos en Europa, Cuadernos constitucionales de la Cátedra Fadrique Furió Ceriol, nº 11-12, 1995.

GARZÓN, I.: "La protección de los datos personales y la función normativa del Consejo de Europa", Revista de Instituciones Europeas, nº 1, 1981.

GRABENWARTER, C.: European Convention on Human Rights. Commentary, Ed. Beck, Hart, Oxford, 2014.

LAFFERTY, M.: "Article 8: The right to respect for private and family life, home, and correspondence", en HARRIS, BOYLE, y WARBRICK, Law of the European Convention on Human Rights, Ed. Oxford University Press, Oxford, 2014.

RENUCCI, J.F.: Droit européen des Droits de l´Homme. Droits et libertés fondamentaux garantis par la CEDH, Ed. LGDJ, Paris, 2015.

PARLAMENTO EUROPEO: "Informe sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos de Interior, nº 2013/2188(INI).

PAVÓN, J. A.: "La protección de datos personales en el consejo de Europa: el protocolo adicional al convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales", Anuario de la Facultad de Derecho, Universidad de Extremadura, nº 19-20, 2002.

PÉREZ DE LOS COBOS, F.: El recurso individual ante el Tribunal Europeo de Derechos Humanos, Ed. Tirant lo Blanch, Valencia, 2018.

SALAMANCA, E.: "El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de las comunicaciones", Revista del Instituto Español de Estudios Estratégicos, nº, 2014.

SUDRE, F.: Droit européen et international des droits de l´homme, Ed. PUF, Paris. 2015.

SUDRE, F. y otros: Les grands arrêts de la Cour européenne des droits de l'homme. Ed. PUF, Paris, 2017.

VILLAVERDE, I.: "Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo", Revista de Derecho Constitucional, nº 41, 1994.

Sitios web consultados

Sitio sobre protección de datos personales del Consejo de Europa: https://www.coe.int/en/web/data-protection

Base de datos de jurisprudencia del TEDH del Consejo de Europa: https://hudoc.echr.coe.int/eng#

Blog especializado en la jurisprudencia del TEDH: https://strasbourgobservers.com/

El presente estudio forma parte de un proyecto más global que pretende poner las bases para poder comparar el régimen jurídico aplicable al derecho al respeto de la vida privada en diferentes ordenamientos jurídicos, así como poder comparar las diferentes soluciones que dichos ordenamientos han previsto para los desafíos que la "era digital" impone a tal derecho.

En este documente se estudia, en lo referido al Consejo de Europa y con respecto al tema que nos ocupa, los convenios en vigor, la jurisprudencia más relevante y la naturaleza del derecho al respeto de la vida privada, acabando con unas conclusiones sobre los desafíos mencionados.

QA-04-18-867-ES-N

Esta es una publicación de la Unidad Biblioteca de Derecho Comparado
EPRS | Servicio de Estudios del Parlamento Europeo

Impreso ISBN 978-92-846-4049-2 | doi:10.2861/539638 | QA-04-18-867-ES-C
PDF ISBN 978-92-846-4040-9 | doi:10.2861/72951 | QA-04-18-867-ES-N