BOLETÍN DEL MINISTERIO DE JUSTICIA

Año LXXVI · Núm. 2.256 · Octubre de 2022

ESTUDIO DOCTRINAL

VIGILANCIA Y ESTADO DE DERECHO

Antonio Gutiérrez Cardenete

GOBIERNO DE ESPAÑA · MINISTERIO DE JUSTICIA

ISSN: 1989-4767
NIPO: 051-15-001-5
https://revistas.mjusticia.gob.es/index.php/BMJ

Enlaces de contacto

Contacto Boletín
Normas de publicación en el Boletín del Ministerio de Justicia

VIGILANCIA Y ESTADO DE DERECHO

ANTONIO GUTIÉRREZ CARDENETE

Letrado de la Administración de Justicia
Punto de contacto de la Red de Cooperación Jurídica Internacional del Ministerio de Justicia
Doctorando del Instituto de Derecho Penal Europeo e Internacional de la Universidad de Castilla-La Mancha

Psychic spies from China try to steal your mind's elation
An' little girls from Sweden dream of silver screen quotation
And if you want these kinds of dreams, it's Californication.

Red Hot Chili Peppers, Californication (1999), Warner Music Group

׃יִכֹנָא יִחָא רֵמֹשֲׁה יִתְּעַדָי אֹל רֶמאֹיַּו ךָיִחָא לֶבֶה יֵא ןִיַק־לֶא הָוהְי רֶמאֹיַּו

Entonces el Señor preguntó a Caín: «¿Dónde está tu hermano Abel?». «No lo sé», respondió Caín. «¿Acaso yo soy el guardián de mi hermano?».

Gn, 4, 9

Resumen

La regulación de la vigilancia resulta esencial en el Estado de derecho, como han demostrado los abusos resultantes de escándalos internacionales como las revelaciones de Edward Snowden sobre las prácticas de la NSA o, más recientemente, en el uso del programa Pegasus *por Gobiernos y agencias de inteligencia. Este estudio analiza los elementos incorporados por la Comisión de Venecia del Consejo de Europa a su lista de control del Estado de derecho a la luz de la jurisprudencia europea y de las recomendaciones de supervisores de protección de datos.*

Palabras clave

Vigilancia, ciberespacio, Estado de derecho, protección de datos, vigilancia estratégica, videovigilancia, reconocimiento facial.

Abstract

The regulation of surveillance is essential for the rule of law as demonstrated by the NSA practices revealed by Edward Snowden or more recently by the allegations of the use of the Pegasus programme by governments and intelligence agencies. This work elaborates on the elements incorporated by the Council of Europe's Venice Commission into its rule of law checklist against the background of European case law and the guidance of data protection supervisors.

Keywords

Surveillance, Cyberspace, Rule of law, Data protection, Strategic surveillance, Video-surveillance, Facial recognition.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

SUMARIO

INTRODUCCIÓN

La vigilancia se define como «el cuidado y atención exacta en las cosas que están a cargo de cada uno o el servicio ordenado y dispuesto para vigilar», que es «observar algo o a alguien atenta y cuidadosamente»[1]. Existe un matiz teleológico en la primera acepción que permite distinguir la vigilancia de la mera curiosidad, del voyerismo o del acecho al proyectar la acción de cuidar y atender sobre sujetos u objetos «a cargo» del vigilante. Resulta así de esta definición una legitimación del vigilante debido a su vinculación o relación con el objeto o sujeto vigilado. Aunque la segunda acepción de la vigilancia se vincula mediatamente a la visión (observar) como sentido predominante en los homínidos[2], lo cierto es que la acción de vigilar puede hacerse extensiva a los otros sentidos que también permiten a nuestro cerebro interpretar cambios en nuestro entorno físico.

La inteligencia humana ha permitido vencer las limitaciones naturales de nuestros sentidos potenciándolos de modo artificial (v. g. prismáticos, micrófonos, etc.) o colocando al sujeto u objeto vigilado en unas condiciones que faciliten este fin[3]. De este modo el ser humano ha incorporado sensores artificiales que van más allá de los sentidos de los que está dotado naturalmente y que le permiten adaptar a sus sentidos limitados lo que de modo natural le es imperceptible (v. g. cámaras de visión infrarroja). Pero el ingenio no solo ha proporcionado un aumento de las capacidades de percepción (de sentir), sino que también ha conseguido aumentar la habilidad para procesar la información recibida y extraer conclusiones o predicciones acerca de la misma mediante el procesamiento automatizado de datos (digitales), que emula y en algunos casos sobrepasa las capacidades del cerebro humano (v. g. el reconocimiento automatizado de objetos o de personas mediante programas informáticos de inteligencia artificial), siendo capaz de interpretar un volumen y variedad de datos a una velocidad que no sería posible de no mediar la facilitación cognitiva que resulta del uso de esta herramienta[4].

En virtud de estas herramientas tecnológicas propias de la sociedad de la información se ha producido una mutación en la relación entre estímulo y percepción relativa a objetos o personas en el mundo físico (cosmos), al haberse generado un nuevo entorno, el digital (cibercosmos)[5], que, si bien depende finalmente de fenómenos

1 RAE, *Diccionario de la lengua española*, «vigilancia» y «vigilar».

2 Colavita, Francis B. (1974). «Human sensory dominance». *Perception & Psychophysics* 16(2), pp. 409-412.

3 Bentham, J. (1787). «Panopticon or the inspection-house».

4 Apud, I. (2014). «¿La mente se extiende a través de los artefactos? Algunas cuestiones sobre el concepto de cognición distribuida aplicado a la interacción mente-tecnología», *Revista de Filosofía de la Universidad Complutense de Madrid*, 39(1).

5 Pau A. y Hernando Grande A. (enero de 2001). «La cibercosmología como premisa del ciberderecho», *Boletín del Ministerio de Justicia*, año LXXV, núm. 2.236.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

físicos (ondas electromagnéticas)[6], de modo inmediato no resulta perceptible por los sentidos naturales, necesitando la intervención humana en el mismo de la intermediación de una máquina.

Esta interfaz hombre-máquina permite diferentes relaciones del cosmos con el cibercosmos, La superposición del cibercosmos al cosmos se ha venido a denominar «realidad aumentada», que permite amplificar la capacidad de vigilancia del espacio físico, añadiendo a la percepción directa del mismo otras capas virtuales de información[7]. En sentido inverso, el ser humano puede emular una experiencia de espacio físico (cosmos) en el cibercosmos mediante interfaces de realidad virtual[8]. De este modo, la vigilancia puede ejercitarse en ambos entornos (el físico y el digital), y en ambos casos la percepción humana puede ser mediatizada por un artefacto. Aún más, el propio sujeto de la acción de vigilar (el vigilante) puede ser automatizado, en cuyo caso no hablaríamos propiamente de percepción humana, aunque la finalidad de la acción del vigilante-máquina sea definida por seres humanos (v. g. un programa antivirus).

La vigilancia puede ejercerse sobre un sujeto o un objeto (vigilancia específica), o de modo general sobre un entorno (vigilancia estratégica). La capacidad de vigilancia del ser humano sobre un entorno depende no solo de su capacidad natural de percepción, sino también de sus limitaciones naturales para procesar la información percibida y tomar decisiones (v. g. no es lo mismo vigilar una oveja en un cercado que vigilar un rebaño disperso en un valle). Del mismo modo, en el entorno virtual no es lo mismo vigilar los datos emitidos o recibidos por un dispositivo particular (v. g. un teléfono móvil) que vigilar en masa la información que transita en un cable intercontinental de fibra óptica o en un satélite de telecomunicaciones.

Existe asimismo una interacción entre el entorno físico y el entorno digital condicionada por la creciente capacidad de este último de expandirse con información (datos) extraídos del primero mediante artefactos «conectados». El llamado «Internet de las cosas» eleva exponencialmente la capacidad de ejercer la vigilancia del entorno físico a través de medios conectados al entorno digital. Por ejemplo, el omnipresente *smartphone* o teléfono inteligente incorpora un amplio arsenal de sensores[9] que lo convierten en un artefacto con un enorme potencial para ser usado con fines de vigilancia.

---

6 De no depender de un fenómeno físico, el ciberespacio sería objeto de estudio por la metafísica.

7 Ejemplos de interfaces de realidad aumentada son las gafas Google Glass o las Microsoft Hololens.

8 Ejemplos de interfaces de realidad virtual son las gafas Oculus de Facebook o las PlayStation VR de Sony.

9 Cámara, micrófono, acelerómetro, giroscopio, sensor de luz ambiental, GPS/GLONASS/GNSS, sensor de proximidad, sensor de huellas dactilares, etc.

Si la dimensión espacial es relevante para la vigilancia, también lo es la dimensión temporal, ya que la técnica también ha permitido mutar la vigilancia tradicional, ejercitada con la percepción directa e inmediata de los sentidos, en una vigilancia retrospectiva (sobre lo que ya ha sucedido) basada en la conservación de la información necesaria para realizar un análisis posterior (v. g. el visionado de la grabación de una videocámara de seguridad). En el entorno digital esta «máquina del tiempo» se basa en la obligación impuesta por el Estado a los proveedores de servicios de conservar o transmitir determinadas categorías de datos de las telecomunicaciones y de ponerlas a disposición de las autoridades. La desmaterialización de la vigilancia retrospectiva se ha conseguido mediante el almacenamiento y procesamiento de datos «en la nube» (*cloud computing*), proceso técnico que reintroduce nuevamente la cuestión de la dimensión espacial, ya que la información no permanece almacenada en un único dispositivo, sino que «circula» entre distintos dispositivos conectados en red y situados en distintas ubicaciones[10]. Sin embargo, el aumento progresivo de la velocidad de procesamiento de datos, unido al desarrollo de la inteligencia artificial, está relativizando la importancia del almacenaje de la información, de modo que nuevas herramientas automatizadas permiten procesar grandes volúmenes de información de manera automatizada en tiempo real. La inteligencia artificial también permite proyectar la acción de vigilancia hacia el futuro, ya que los algoritmos realizan predicciones cada vez más exactas sobre muy diversos escenarios de riesgo permitiendo optimizar los recursos materiales y humanos dedicados a esta actividad (v. g. aplicaciones policiales sobre zonas y horarios de mayor incidencia de la criminalidad en una ciudad, predicción de riesgo en asuntos de violencia sobre la mujer, etc.), si bien existe un claro riesgo de que los algoritmos reproduzcan prejuicios que puedan dar como resultado la discriminación de determinadas áreas o sectores sociales[11].

El ciberespacio está sujeto a las mismas tensiones y rivalidades estratégicas que el mundo físico, aunque sus dimensiones y consecuencias son diferentes:

En el mundo analógico, la existencia de un arma de guerra es manifiesta; sin embargo, en el ciberespacio, la existencia de un arma de ciberguerra no se diferencia sustancialmente del resto del tráfico pacífico de datos, y de hecho se programan con esta finalidad. Por ejemplo, no es posible comparar la presencia de un carro blindado en un hospital con la de un *software* malicioso (*malware*) diseñado para destruir infraestructuras críticas, ya que este último sí puede pasar desapercibido entre los programas informáticos de un servicio público de salud.

---

10 Un análisis detallado de los retos de la computación en la nube para la investigación criminal se contiene en el informe del Comité del Convenio de Budapest del Consejo de Europa (2015). Criminal justice access to data in the cloud: challenges. Este informe ha inspirado algunos de los cambios introducidos en los mecanismos de cooperación internacional para la obtención de prueba electrónica introducidos en el 2.º protocolo adicional del citado Convenio de Budapest.

11 FRA (2018). Guía para prevenir la elaboración ilícita de perfiles en la actualidad y en el futuro, capítulo 3.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

Si estalla un conflicto armado en el entorno físico, existen instrumentos de derecho humanitario limitadores de la acción bélica en evitación de daños a la población civil; sin embargo, el entorno digital es un inmenso campo de batalla en el que transitan de modo cotidiano civiles, igualmente vulnerables frente a un ciberataque que puede producir consecuencias aún más fatales que las derivadas del uso de armas analógicas, porque muchas infraestructuras críticas dependen de modo cotidiano de su conexión con el ciberespacio, resultando un daño indiscriminado en la población civil[12]. Así, siguiendo con el anterior ejemplo, el uso de un carro blindado contra un hospital puede dar lugar a un crimen de guerra manifiesto, pero de consecuencias limitadas a dicho hospital; sin embargo, la destrucción de los sistemas críticos de un servicio público de salud (sistemas automatizados de gestión de historiales médicos, de unidades de cuidados intensivos, de recursos humanos, de materiales y medicamentos, etc.) puede ocasionar un número de bajas civiles considerablemente mayor, por la escala y la velocidad con que dicho ataque puede tener lugar.

A nivel global, la Asamblea General de la Organización de las Naciones Unidas (ONU) ha constituido desde el año 2003 Grupos de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional[13]. Una de las principales conclusiones de estos trabajos, asumida por la Asamblea General de la ONU, es que el derecho internacional y los derechos humanos son igualmente aplicables a la esfera digital: no se trata pues de crear nuevos valores o principios jurídicos para el ciberespacio, sino de adaptar los mecanismos que habilitan su aplicación y garantía tanto en la esfera física como en la digital. Debido al condicionamiento del ciberespacio como «zona de guerra» la prioridad de los Estados es vigilarlo con medios proporcionales a los riesgos y amenazas existentes, resultando así una necesidad de flexibilizar las garantías protectoras de los derechos y libertades civiles cuando la vigilancia tiene como objeto la protección de la seguridad nacional[14].

El aumento en la intensidad de la vigilancia no solo tiene su efecto inmediato en el ejercicio de derechos y libertades fundamentales de los individuos, sino que de modo mediato puede condicionar los propios valores fundacionales de todo ordenamiento jurídico, entre los que se encuentra el Estado de derecho (EdD), que se define como «[la] organización política de la comunidad orientada a la limitación del poder para preservar una esfera autónoma de acción y de realización a los ciudadanos»; como «[un] valor común a la UE y a sus Estados miembros»; y como «[aquel] requisito que

12 Organización de Naciones Unidas (2021). Informe del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional; A/76/135.

13 Resoluciones de la Asamblea General de la ONU A/RES/58/32, A/RES/60/45, A/RES/66/24, A/RES/68/243, A/RES/70/237 y A/RES/73/266.

14 Un buen ejemplo puede encontrarse en el doble estándar fijado en la doctrina del TJUE respecto a la vigilancia masiva de datos en las sentencias de los asuntos Big Brother Watch y otros, y La Quadrature du Net y otros.

debe reunir un Estado europeo para ingresar en el Consejo de Europa y en la Unión Europea»[15], si bien estas instituciones europeas prefieren acudir a una descripción del EdD mediante los principios que lo integran: legalidad, seguridad jurídica, prohibición de la arbitrariedad del poder ejecutivo, tutela judicial efectiva, separación de poderes e igualdad ante la ley[16].

El EdD viene referido a la comunidad o a la sociedad en su conjunto, y por ello la exigencia de respeto a los principios que lo componen se predica tanto de las autoridades como de los particulares[17]. La vigilancia por las autoridades tiene como fines principales la lucha contra la criminalidad y la protección de la seguridad nacional, aunque por la reciente pandemia del virus COVID-19 también ha adquirido relevancia la vigilancia epidemiológica.

Debido a que el desarrollo del ciberespacio y de las telecomunicaciones ha dependido principalmente de la iniciativa privada de grandes empresas tecnológicas multinacionales, se ha introducido un giro inesperado en el relato tradicional de la influencia de la vigilancia en el EdD. Este relato venía tradicionalmente marcado por la experiencia de estados policiales consecuencia de regímenes políticos iliberales (comunismo y fascismo)[18]. Sin embargo, la realidad ha demostrado que las mismas grandes multinacionales que han contribuido al desarrollo del ecosistema digital son las que han basado su modelo de negocio en la vigilancia y explotación de los datos personales de sus usuarios, todo ello en connivencia con Estados basados formalmente en regímenes políticos liberales[19]. Según el Supervisor Europeo de Protección de Datos (SEPD): «En los últimos años, también hemos sido testigos de cómo varias empresas del sector privado han amasado una riqueza, una influencia y un poder político inimaginables, que en el pasado solo se asociaban a los Estados-nación. La mayoría de las veces, esa riqueza y ese poder están directamente relacionados con su capacidad de acumular datos, incluida la información personal, a una escala como nunca fue posible (en clara oposición al principio de minimización de datos). Esto, a su vez, presenta a los Gobiernos y Parlamentos de todo el mundo el reto de cómo ejercer sus poderes soberanos en un ámbito monopolizado por los imperativos del beneficio

15 RAE, Diccionario *panhispánico del español jurídico*, «Estado de derecho».

16 Reglamento (UE, Euratom) 2020/2092 del Parlamento Europeo y del Consejo de 16 de diciembre de 2020, sobre un régimen general de condicionalidad para la protección del presupuesto de la Unión. ELI: https://eur-lex.europa.eu/eli/reg/2020/2092/ojhttp://data.europa.eu/eli/reg/2020/2092/oj, considerando (3) y artículo 2 (a). sobre el concepto del Estado de derecho también reflexiona la obra del autor Estado de derecho y derechos fundamentales en la Unión Europea; BMJ núm. 2238 (2021) Tomo LXXXV, Estudios doctrinales.

17 Informe sobre el Estado de derecho, CDL-AD(2011)003rev-e, adoptado por el pleno de la Comisión de Venecia del Consejo de Europa los días 25 y 26 de marzo de 2011, párrafos 16, 36 y 39.

18 Orwell, G. *1984* y Von Donnersmarck, F. H.; *La vida de los otros*.

19 Zuboff, S. (2019) *La era del capitalismo de la vigilancia*, Paidós.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

privado. En mi opinión, este podría ser uno de los mayores desafíos al que los responsables políticos se enfrentan hoy en día, un reto del Estado de derecho, y estoy convencido de que la imposición de límites al volumen de datos sobre las personas que estas empresas están autorizadas a procesar es la clave para resolver este desafío»[20].

La Comisión de Venecia del Consejo de Europa desarrolló una lista de control sobre el EdD en la que incluye a la vigilancia, junto a la corrupción, como uno de los desafíos actuales particularmente relevantes para el EdD[21]. El presente estudio aborda la influencia de la vigilancia sobre el EdD a través de los cuatro factores analizados en dicha lista de control: la recolección y tratamiento de datos personales, la vigilancia específica, la vigilancia estratégica y la videovigilancia.

I. Garantías relativas a la recolección y tratamiento de datos personales para la vigilancia

La vigilancia sobre uno o varios sujetos implica el tratamiento de datos de carácter personal, que son toda información sobre una persona física identificada o identificable (el interesado)[22]. Este tratamiento puede causar distintos niveles de injerencia en un derecho fundamental consagrado en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE)[23] y también comprendido en el derecho humano a la vida privada personal y familiar del artículo 8 del Convenio Europeo de Derechos Humanos (CEDH)[24].

La lista de control del EdD opta por centrar su atención en la protección de datos, al ser este un derecho más amplio que el de la vida privada (reconocido en un artículo separado —el 7— de la CDFUE): la tutela ofrecida por el artículo 8 CDFUE afecta al tratamiento de todo tipo de datos personales, sin perjuicio de la eventual afectación de la vida privada y familiar[25]. En la medida en que el tratamiento de datos personales afecta a la esfera privada del individuo, también entrará en juego la tutela del derecho a la intimidad (artículo 7 CDFUE). De igual modo, el ejercicio de libertades públicas esenciales para la democracia, como la de pensamiento, conciencia y religión (artículo 10 CDFUE), la de expresión y de información (artículo 11 CDFUE), o la de reunión y

20 Traducción por el autor de extracto del discurso de SEPD el 19 de septiembre de 2022; Mentor Group Forum for EU-US Legal Economic Affairs; accesible en https://edps.europa.eu/system/files/2022-09/22-09-19_speech_ww_mentor_group_en.pdf.

21 Consejo de Europa, Comisión de Venecia, «Rule of law checklist» aprobada por el pleno de 11-12 de marzo de 2016; CDL-AD(2016)007rev, apartado F (2).

22 Artículos 4.1 RGPD y 8 del Convenio STCE n.º 108+.

23 Carta de los Derechos Fundamentales de la Unión Europea; ELI: http://data.europa.eu/eli/treaty/char_2016/oj.

24 Consejo de Europa, Convenio para la protección de los derechos humanos y las libertades fundamentales firmado en Roma, el 4 de noviembre de 1950; STCE n.º 5.

25 FRA (2018). Manual de legislación europea en materia de protección de datos, pp. 20-24.

asociación (artículo 12 CDFUE), pueden verse socavadas por la percepción social de que cualquier acto o comunicación está siendo objeto del escrutinio permanente y omnímodo de las autoridades[26]. El TJUE ha destacado que la libertad de expresión constituye uno de los fundamentos esenciales de una sociedad democrática y pluralista y forma parte de los valores en los que se basa la Unión, con arreglo al artículo 2 TUE[27].

1. Principios generales de la protección de datos personales y retos específicos en el ámbito de la vigilancia

La lista de control sobre el EdD enumera las garantías respecto a la recolección y procesamiento de datos personales, en la vigilancia, incluidas las realizadas con fines de protección de la seguridad nacional. Dichas garantías se enmarcan en el desarrollo de la protección del derecho fundamental a la protección de datos personales, tanto en el ámbito del Consejo de Europa (con el Convenio del Consejo de Europa para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal —Convenio 108+—[28]) como en el de la Unión Europea (principalmente a través del Reglamento General de Protección de datos —RGPD—[29])[30].

Las garantías europeas comprenden unos principios básicos relativos al tratamiento de datos personales: licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad[31].

Sin embargo, existen aspectos de la regulación europea de la protección de datos que presentan una gran complejidad cuando se abordan desde la perspectiva de la vigilancia. Por un lado, la regulación de la UE y la del Consejo de Europa difieren en su alcance, ya que la primera presenta limitaciones constitucionales en determinados ámbitos vedados a la acción de la UE, como la seguridad nacional. Por otro lado, y aun cuando existe una gran correspondencia entre las disposiciones modernizadas en materia de protección de datos del Consejo de Europa y las de la UE, este marco

26 FRA (2018) Manual de legislación europea en materia de protección de datos, capítulo 1.3

27 STJUE (Gran Sala) de 5 de abril de 2022 en el asunto C-140/20 G.D. y Commissioner of An Garda Síochána; ECLI:EU:C:2022:258; apartado 43.

28 Consejo de Europa, Convenio 108+ en su versión modificada por protocolo de 18 de mayo de 2018.

29 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos); ELI: http://data.europa.eu/eli/reg/2016/679/oj.

30 Agencia de Derechos Fundamentales de la Unión Europea (FRA); «Manual de legislación europea en materia de protección de datos»Edición de 2018; doi:10.2811/60145.

31 Artículos 5 RGPD y 2 a) del Convenio STCE n.º 108+; Rule of Law checklist CDL-AD (2016)007rev, apartado F (2) a) (i).

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

jurídico de garantías tiene aún como reto «acompañar» a los datos europeos cuando son tratados fuera de la jurisdicción europea.

a) Vigilancia y seguridad nacional

En el ámbito del Consejo de Europa, el Convenio 108+ se aplica a los tratamientos de datos personales realizados en los sectores público y privado, incluyendo los realizados con fines relativos a la seguridad nacional[32]. Sin embargo, en el ámbito de la Unión Europea, el artículo 4 (2) TUE dispone que «[La Unión] respetará las funciones esenciales del Estado, especialmente las que tienen por objeto garantizar su integridad territorial, mantener el orden público y salvaguardar la seguridad nacional. En particular, la seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro»[33].

El TJUE, con ocasión del análisis de la legalidad de medidas de conservación de datos en el asunto La Quadrature du Net y otros, ha realizado una primera aproximación teleológica al concepto de seguridad nacional: «Esta responsabilidad corresponde al interés primordial de proteger las funciones esenciales del Estado y los intereses fundamentales de la sociedad, e incluye la prevención y la represión de actividades que puedan desestabilizar gravemente las estructuras constitucionales, políticas, económicas o sociales fundamentales de un país, y, en particular, amenazar directamente a la sociedad, a la población o al propio Estado, tales como las actividades terroristas»[34].

Resulta novedoso que el TJUE aborde la cuestión de la seguridad nacional, no solo en su faceta conceptual, sino también en su caracterización como un objetivo prioritario a la hora de establecer limitaciones a los derechos fundamentales, afirmando que «la importancia del objetivo de protección de la seguridad nacional [...] supera la de los demás objetivos contemplados en el artículo 15, apartado 1, de la Directiva 2002/58, en particular, de los objetivos de combatir la delincuencia en general, incluso grave, y de protección de la seguridad pública. En efecto, amenazas como las mencionadas en el apartado anterior se distinguen, por su naturaleza y especial gravedad, del riesgo general de que surjan tensiones o perturbaciones, incluso graves, que afecten a la seguridad pública. Por lo tanto, sin perjuicio del cumplimiento de los demás requisitos establecidos en el artículo 52, apartado 1, de la Carta, el objetivo de protección de la seguridad nacional puede justificar medidas que supongan injerencias en los derechos fundamentales más graves que las que podrían justificar esos otros objetivos»[35].

---

32 Consejo de Europa, Convenio 108+, artículo 3 (1).

33 Tratado de la Unión Europea, versión consolidada, 2016/C/202/01.

34 STJUE (Gran Sala) de 6 de octubre de 2020 en los asuntos acumulados La Quadrature du Net y otros contra Premier ministre y otros; ECLI:EU:C:2020:791; apartado 135.

35 *Ibid.,* apartado 136.

A diferencia de la delincuencia, aunque sea especialmente grave, una amenaza para la seguridad nacional debe ser real y actual, o cuando menos previsible, lo que supone que surjan circunstancias suficientemente concretas para poder justificar una medida de conservación generalizada e indiferenciada de datos de tráfico y de localización, durante un plazo limitado. Así pues, tal amenaza se distingue, por su naturaleza, su gravedad y el carácter específico de las circunstancias que la forman y del riesgo general y permanente de que surjan tensiones o perturbaciones, incluso graves, que afecten a la seguridad pública, o del riesgo de delitos graves. La delincuencia, aunque sea especialmente grave, no puede asimilarse, pues, a una amenaza para la seguridad nacional porque tal asimilación podría implicar la introducción de una categoría intermedia entre la seguridad nacional y la seguridad pública para aplicar a la segunda las exigencias inherentes a la primera[36].

No existe duda sobre la aplicación de la normativa de protección de datos de la UE a las acciones de vigilancia efectuadas por actores privados, pero existen matices cuando esta tiene por objeto la salvaguardia de la seguridad nacional. Concretamente, el TJUE (ha debido pronunciarse en el asunto *Privacy International y otros*[37] sobre la aplicabilidad de la normativa europea de protección de datos personales y de privacidad de las comunicaciones electrónicas a aquellos supuestos en los que la normativa nacional imponía a los prestadores de servicios de comunicaciones electrónicas la conservación o facilitación del acceso en tiempo real de los datos de tráfico y localización a los servicios de inteligencia).

En el juicio, nueve Gobiernos de los Estados miembros se opusieron a la aplicación de la Directiva 2002/58 (también llamada Directiva de privacidad de las comunicaciones electrónicas). En primer lugar, el TJUE recordó que, aunque el apartado primero del artículo 15 de la Directiva se refiere a actividades propias de las autoridades, tales como la salvaguarda de la seguridad nacional y la lucha contra la delincuencia, dichas medidas regulan, a los efectos mencionados en dicha disposición, la actividad de los proveedores de servicios de comunicaciones electrónicas. Por lo tanto, en la medida en que regulan la actividad de dichos operadores privados no pueden asimilarse a actividades propias de los Estados, que son las expresamente excluidas del ámbito de aplicación de la Directiva en su artículo 1 (3)[38].

En segundo lugar, los Gobiernos argumentaron que las disposiciones del artículo 3 (1) de la Directiva 2002/58 y del artículo 3 (2) de la Directiva 95/46 reflejan el reparto de competencias previsto en el artículo 4 TUE (Tratado de la Unión Europea), apartado 2, y quedarían privadas de eficacia si las medidas comprendidas en el ámbito de la

36 STJUE (Gran Sala) de 5 de abril de 2022 en el asunto C-140/20 G.D. contra Commissioner of the Garda Síochána y otros, ECLI:EU:C:2022:258, apartados 62 y 63.

37 Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2020 en el asunto C-623/17 Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, ECLI:EU:C:2020:790.

38 *Ibid.*, apartado 39.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

seguridad nacional tuvieran que respetar los requisitos de la Directiva 2002/58. La Gran Sala, también desestima este argumento al fijar que, si bien corresponde a los Estados miembros determinar sus intereses esenciales de seguridad y adoptar las medidas adecuadas para garantizar su seguridad interior y exterior, el mero hecho de que se haya adoptado una medida nacional con el fin de proteger la seguridad nacional no puede dar lugar a la inaplicabilidad del Derecho de la Unión ni dispensar a los Estados miembros de la necesaria observancia de dicho Derecho[39].

Los Gobiernos personados invocaron, finalmente, la jurisprudencia relativa a la actividad de suministro de datos por las aerolíneas relativos al registro de pasajeros[40], pero este precedente también fue desestimado por el TJUE al considerar que el ámbito de exclusión de la Directiva 95/46 era más amplio que el de la Directiva 2002/58, ya que esta última sí comprende el conjunto de tratamientos de datos personales efectuados por los proveedores de servicios de comunicaciones electrónicas, incluidos los tratamientos que se derivan de las obligaciones que les imponen los poderes públicos. Además, el artículo 23, apartado 1, letras d) y h) del RGPD, impone una nueva lectura al tratamiento en función del tipo (público o privado) del responsable, ya que el efectuado por particulares con fines de prevención y detección de infracciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención, a diferencia de la Directiva 95/46, ahora está comprendido en el ámbito de aplicación del RGPD[41].

Esta doctrina del TJUE resulta relevante porque clarifica la aplicabilidad de la normativa de privacidad de las comunicaciones electrónicas de la Unión a aquellas actividades de conservación o transmisión de datos realizadas por operadores privados pero que redundan en finalidades propias de las autoridades, como vigilancia relativa a la seguridad nacional y la lucha contra la criminalidad[42]. En cambio, cuando los Estados miembros aplican directamente medidas que suponen excepciones a la confidencialidad de las comunicaciones electrónicas, sin imponer obligaciones de tratamiento a los proveedores de servicios de tales comunicaciones, las medidas en cuestión deben cumplir en particular el Derecho nacional de rango constitucional y las exigencias del CEDH[43].

---

39 *Ibid.*, apartado 44 y jurisprudencia precedente de 4 de junio de 2013, ZZ, C-300/11, EU:C:2013:363, apartado 38 y jurisprudencia citada; de 20 de marzo de 2018, Comisión/Austria (Imprenta del Estado), C-187/16, EU:C:2018:194, apartados 75 y 76, y de 2 de abril de 2020, Comisión/Polonia, Hungría y República Checa (Mecanismo temporal de reubicación de solicitantes de protección internacional), C-715/17, C-718/17 y C-719/17, EU:C:2020:257, apartados 143 y 170.

40 STJUE (Gran Sala) 30 de mayo de 2006, Parlamento/Consejo y Comisión (C-317/04 y C-318/04, EU:C:2006:346.

41 *Ibid.*, apartado 47.

42 *Ibid.*, apartado 49.

43 *Ibid.*, apartado 48.

b) Vigilancia interior y vigilancia exterior: el problema de las transferencias internacionales de datos personales

El segundo problema relacionado con la vigilancia de las comunicaciones electrónicas está condicionado por las transferencias internacionales de datos efectuadas por los proveedores de servicios de comunicaciones electrónicas. La asimetría en la tutela de la privacidad y de la protección de datos personales dentro y fuera de Europa choca frontalmente con la arquitectura global del Internet y de las comunicaciones electrónicas. Así, el centro de la discusión actual no radica tanto en definir los valores y principios europeos de la protección de datos y de la privacidad como en hacerlos efectivos en la práctica, evitando que la normativa europea quede en un intento fútil de poner puertas al campo.

La configuración de las transferencias internacionales de datos personales en el Derecho derivado de la UE y en el Convenio STCE 108+ tiene como factor común la necesidad de asegurar un nivel de protección adecuado[44]. Es decir, los «datos personales europeos» no pueden ser exportados fuera de la jurisdicción salvo que viajen acompañados por el nivel de protección que les otorga la normativa europea.

La propia noción de transferencia internacional, como un tipo de tratamiento de datos personales, ha debido ser objeto de interpretación por el TJUE[45]. Sobre esta base interpretativa, el CEPD (Comité Europeo de Protección de Datos) ha publicado unas Directrices sobre la relación entre el artículo 3 RGPD (ámbito de aplicación territorial del RGPD) y el capítulo V (transferencias internacionales)[46] de modo que requiere:

1.º Que un responsable o encargado del tratamiento (exportador) esté vinculado por el RGPD en los términos del artículo 3 y de las Directrices 3/2018 sobre el ámbito de aplicación territorial del RGPD[47].

2.º Que el responsable o encargado del tratamiento transmita o ponga a disposición los datos personales a otro responsable o encargado (el importador)[48].

3.º Que el importador esté en un tercer país o sea una organización internacional, sin perjuicio de que le sea aplicable al mismo el RGPD.

---

44 RGPD, artículo 44 (el nivel de adecuación debe interpretarse de modo que se asegure que el nivel de protección garantizado por el Reglamento no se vea menoscabado); Convenio STCE n.º 108+ artículo 14 (2) y (3).

45 TJUE, C-101/01, Sentencia del Tribunal de Justicia de 6 de noviembre de 2003. Procedimento penal entablado contra Bodil Lindqvist. ECLI:EU:C:2003:596, apartados 56 a 71.

46 CEPD, «Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR».

47 CEPD, Directrices 3/2018 relativas al ámbito territorial del RGPD (artículo 3).

48 Teniendo en cuentas las Directrices 7/2020 del CEPD sobre los conceptos de responsable y encargado del tratamiento.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

El ámbito de la transferencia internacional de datos personales está muy vinculado al ejercicio de la soberanía y la capacidad para tutelar efectivamente su protección durante y tras la propia transferencia. En el asunto *Schrems II*[49] el TJUE fue más allá de las conclusiones efectuadas en el asunto *Privacy International y otros*[50] al abordar la posible interceptación por los servicios de inteligencia estadounidenses de las comunicaciones electrónicas (transferencias internacionales de datos) a Facebook Inc. desde su filial europea Facebook Ireland Ltd.

El tribunal afirmó que está comprendida dentro del ámbito de aplicación del RGPD una transferencia de datos personales realizada con fines comerciales por un operador económico establecido en un Estado miembro a otro operador económico establecido en un país tercero, a pesar de que, en el transcurso de esa transferencia o tras ella, esos datos puedan ser tratados por las autoridades del país tercero en cuestión con fines de seguridad nacional, defensa y seguridad del Estado. Por lo tanto, el TJUE extiende la protección otorgada por el marco europeo incluso en supuestos en los que la acción de injerencia es realizada directamente por un servicio de inteligencia de un tercer Estado, y no por la colaboración de un proveedor de servicios privado (en virtud de una obligación de conservar o transmitir los datos). La base jurídica de esta extensión es que la limitación prevenida en al artículo 4 (2) TUE relativa a la seguridad nacional solo viene referida a los Estados miembros, y no a terceros Estados[51].

En el ámbito de la UE, una de las principales garantías para la transferencia internacional de datos personales es la existencia de una «decisión de adecuación» adoptada por la Comisión Europea, en virtud de la cual se considera que un país o un territorio específico de un tercer país o una organización internacional garantizan un nivel de protección adecuado. Este tipo de decisiones requiere un proceso de evaluación previa por la Comisión cuyo primer elemento para tener en cuenta es el nivel de cumplimiento del EdD[52] en el país destinatario de datos personales europeos.

Teniendo en cuenta que gran parte de los proveedores globales de servicios de la sociedad de la información son compañías estadounidenses, la decisión de adecuación de los EE. UU. ha sido objeto de un intenso escrutinio bajo los criterios de la normativa de protección de datos de la UE, hasta el punto de que la decisión de adecuación de

---

49 TJUE, C-311/18, Sentencia del Tribunal de Justicia (Gran Sala) de 16 de julio de 2020 Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, ECLI:EU:C:2020:559.

50 Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2020 en el asunto C-623/17 Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, ECLI:EU:C:2020:790.

51 *Ibid*. apartados 81 y 89.

52 RGPD, artículo 45.2.a), RGPDUE, artículo 47.1 y Directiva (UE) 680/2016, artículo 36.2.a). La Comisión Europea mantiene un listado actualizado de terceros países respecto de los cuales ha dictado decisión de adecuación.

este país ha sido invalidada en dos ocasiones por el TJUE en los asuntos *Schrems I*[53] y *Schrems II*[54], al apreciar deficiencias en la evaluación de adecuación efectuada por la Comisión Europea. Las deficiencias tenían relación directa con las garantías de los datos europeos (tratados por Facebook) frente a la normativa estadounidense reguladora del acceso a dichos datos por parte de determinados programas de vigilancia para la seguridad nacional de los EE. UU.

En *Schrems I* el TJUE evidenció que la Comisión había incumplido su deber de otorgar seguridad jurídica a las transferencias internacionales de datos personales, ya que en su Decisión 2000/520[55] no manifestó que Estados Unidos garantice efectivamente un nivel de protección adecuado debido a su legislación interna o sus compromisos internacionales. En efecto, el Anexo I, párrafo 4.º, de la Decisión reconocía la primacía de las exigencias de seguridad nacional, interés público y cumplimiento de la ley [de Estados Unidos] sobre los principios rectores de protección de datos de la propia Decisión; y por lo tanto permitía el acceso generalizado por las autoridades estadounidenses al contenido de las comunicaciones electrónicas lesionando el contenido esencial del derecho fundamental a la respecto de la vida privada, sin que el marco legal estadounidense habilitara ninguna posibilidad de que el interesado ejercite acciones frente a dicha intromisión, lesionando así la esencia del derecho a la tutela judicial efectiva, inherente a la existencia del EdD[56]. Además, la Comisión excedió su competencia al incorporar en el artículo 3 de la Decisión restricciones a los poderes de las autoridades de control europeas, privándolos de las facultades necesarias para hacer efectivos los derechos invocados por interesados sujetos a dichas transferencias internacionales a los EE. UU.[57].

En *Schrems II*, la nueva Decisión de adecuación sí contenía una garantía expresa por parte de la Comisión Europea de que los Estados Unidos garantizaban un nivel adecuado de protección de los datos personales transferidos desde la UE a entidades

53 TJUE, C-362/14, Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015, Maximillian Schrems contra Data Protection Commissioner, ECLI:EU:C:2015:650.

54 TJUE, C-311/18, Sentencia del Tribunal de Justicia (Gran Sala) de 16 de julio de 2020, Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, ECLI:EU:C:2020:559.

55 Decisión de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. ELI: http://data.europa.eu/eli/dec/2000/520/oj.

56 TJUE, C-362/14, Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015, Maximillian Schrems contra Data Protection Commissioner, ECLI:EU:C:2015:650, apartados 94 a 97.

57 TJUE, C-362/14, Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015, Maximillian Schrems contra Data Protection Commissioner, ECLI:EU:C:2015:650, apartados 99 a 105.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

establecidas en ese país tercero en el marco del Escudo de la Privacidad UE-EE. UU. Sin embargo, nuevamente el TJUE declaró inválida esta Decisión porque la evaluación efectuada por la Comisión, en especial sobre al alcance y garantías en la ejecución de los programas de la inteligencia estadounidense, resultó errónea: El TJUE declaró que la normativa estadounidense no satisfacía las exigencias mínimas establecidas por el Derecho de la Unión con respecto al principio de proporcionalidad, de modo que no puede considerarse que los programas de vigilancia basados en esas disposiciones se limiten a lo estrictamente necesario[58]. Aún más, la nueva Decisión perseveraba en el error ya denunciado en *Schrems I* de no salvaguardar la esencia del derecho a la tutela judicial efectiva, ya que el nuevo acuerdo no contenía ninguna indicación de que la figura del defensor del pueblo prevista en el acuerdo con los EE. UU. estuviera facultada para adoptar decisiones vinculantes con respecto a esos servicios ni tampoco menciona ninguna garantía legal que acompañe a ese compromiso y pueda ser invocada por los interesados[59].

La ausencia de una Decisión de adecuación no impide la transferencia internacional de datos personales, ya que existen otras garantías adecuadas para mantener un nivel de protección sustancialmente equivalente al garantizado por la Unión. El mecanismo de garantía más usado por los operadores privados es el de las cláusulas contractuales tipo, que se encuentra recogido en el artículo 46 (2) (c) y (d) RGPD. En el caso de las transferencias de datos a los EE. UU., el TJUE analizó la Decisión relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países[60], concluyendo que esta Decisión prevé mecanismos efectivos que permiten en la práctica garantizar que la transferencia a un país tercero de datos personales sobre la base de las cláusulas tipo de protección de datos recogidas en el anexo de la antedicha Decisión se prohíba o suspenda cuando el destinatario de la transferencia no cumpla las referidas cláusulas o no le resulte posible cumplirlas[61].

---

58 TJUE, C-311/18, Sentencia del Tribunal de Justicia (Gran Sala) de 16 de julio de 2020, Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, ECLI:EU:C:2020:559, apartados 184 y 185.

59 TJUE, C-311/18, Sentencia del Tribunal de Justicia (Gran Sala) de 16 de julio de 2020, Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, ECLI:EU:C:2020:559, apartados 196 y 197.

60 Decisión de la Comisión 2010/87/UE, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46 (DO 2010, L 39, p. 5), en su versión modificada por la Decisión de Ejecución (UE) 2016/2297 de la Comisión, de 16 de diciembre de 2016 (DO 2016, L 344, p. 100).

61 TJUE, C-311/18, Sentencia del Tribunal de Justicia (Gran Sala) de 16 de julio de 2020, Data Protection Commissioner contra Facebook Ireland Limited y Maximillian Schrems, ECLI:EU:C:2020:559, apartados 148 y 149.

Otra faceta de la transferencia internacional de datos personales producto de la vigilancia resulta del intercambio de información entre servicios de inteligencia de países europeos y de terceros Estados[62]. El problema de los acuerdos de intercambio de inteligencia radica en la existencia de lagunas jurídicas consecuencia del carácter secreto de los intercambios de información de inteligencia y de la generalidad de sus previsiones en orden a la existencia de una adecuada supervisión. Dichas lagunas tienen como consecuencia más evidente el riesgo de que los Estados obtengan mediante cooperación internacional la información que les veda su propio marco legal por ser producto de la vigilancia de terceros Estados no sujetos a las mismas garantías.

El TEDH en el asunto *Big Brother Watch y otros c. Reino Unido* dio por buenas las garantías de exportación de datos de inteligencia a terceros países fijadas en su Código de Interceptación de Comunicaciones, que en su apartado 7.5 impone a los servicios de inteligencia adoptar las medidas adecuadas para garantizar que las autoridades de terceros países tengan y mantengan los procedimientos necesarios para salvaguardar el material interceptado y que el mismo solo sea entregado, copiado, distribuido o conservado lo mínimamente imprescindible. Esta norma también prohíbe ulteriores transmisiones a otros países por las autoridades receptoras salvo acuerdo expreso del servicio de inteligencia nacional remitente, y que se proceda a la devolución o destrucción segura del material cuando ya no sea necesario. El apartado 4.30 del Código de Interceptación de Comunicaciones también establece una política de marcado del material como confidencial y que si existiera cualquier duda sobre la legalidad de la diseminación de este material se proceda de modo obligatorio a elevar consulta a un asesor legal de la agencia de inteligencia[63]. Sin embargo, aunque el criterio del TEDH viene referido a la exportación de datos de inteligencia a terceros países, aún no existe una referencia jurisprudencial sobre las garantías necesarias que adoptar sobre la importación de datos producto de la vigilancia de terceros países, que paradójicamente puede derivar de acciones de vigilancia sobre individuos en jurisdicción europea que han sido obtenidos por terceros Estados con métodos incompatibles con los estándares de orden público europeo.

Por el contrario, la Gran Sala dictaminó en la sentencia gemela del asunto *Centrum för rättvisa c. Suecia*[64] que el sistema sueco de exportación de inteligencia no cumplía los requisitos mínimos de legalidad, ya que la normativa sueca no disponía de modo explícito el requisito previo de ponderación de la necesidad y proporcionalidad de

62 Por ejemplo, la comunidad de inteligencia europea SIGINT Seniors Europe, integrada a su vez por la Comunidad de Inteligencia Five Eyes (EE. UU., R. U., Canadá, Australia y Nueva Zelanda) y por Francia, Alemania, Italia, España, Bélgica, Países Bajos, Dinamarca, Noruega y Bélgica. FRA (2017). Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update, nota a pie de página n.º 172.

63 STEDH (Gran Sala) de 25 de mayo de 2021 en los asuntos acumulados Big Brother Watch y otros c. Reino Unido, ECLI:CE:ECHR:2021:0525JUD005817013, apartados 395 a 399.

64 STEDH (Gran Sala) de 25 de mayo de 2021 en el asunto Centrum för rättvisa c. Suecia, n.º 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, apartado 326.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

compartir con terceras partes la información obtenida, ni de una comprobación previa de la existencia de unas mínimas garantías en el destinatario extranjero de esta información.

El Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Sr. Martin Scheinin, en su informe al Consejo de Derechos Humanos de la ONU en 2010 recopiló buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional que permitan garantizar el respeto de los derechos humanos por los servicios de inteligencia en la lucha contra el terrorismo, particularmente en lo que respecta a su supervisión, y que incluyen garantías específicas para el intercambio de información entre servicios de inteligencia[65].

La Agencia de Derechos Fundamentales de la UE (FRA) recomienda que los Estados miembros de la UE deben establecer marcos legales reguladores de la cooperación internacional en materia de inteligencia que claramente definan la competencia de organismos supervisores en esta materia, que deben quedar exentos de la regla de exclusión de terceros (*third-party rule*) en virtud de la cual se prohíbe compartir los datos procedentes de otra agencia extranjera sin la autorización expresa de esa fuente[66].

2. Transparencia y vigilancia

El principio de transparencia en el tratamiento de datos personales se garantiza con una serie de informaciones sobre el tratamiento que deben ser accesibles para el interesado[67]. Sin embargo, el derecho fundamental a la protección de datos de carácter personal puede ser objeto de limitaciones:

En el ámbito de la UE, el artículo 52 (1) de la CDFUE dispone que «cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, solo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás».

En el ámbito del Consejo de Europa también el párrafo 2.º del artículo 8 del CEDH regula las condiciones generales limitativas de este derecho: «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,

65 ONU, documento A/HRC/14/46, véanse en especial las prácticas 31 a 35.

66 FRA (2018). Opinions Surveillance (vol.II), n.º 9, 10 y 11.

67 Artículos 13 y 14 RGPD; artículo 11.1. a) del Convenio STCE n.º 108+ y Lista de control del EdD CDL-AD (2016)007rev, apartado F (2) a) (ii).

el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

Así, por ejemplo, en el ámbito de la UE los derechos de transparencia y acceso de los interesados pueden ser limitados cuando el fin del tratamiento de datos personales responda a la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención[68], y a tal efecto el legislador de la UE habilita esta limitación mediante disposiciones específicas en la Directiva 680/2016[69] y en el Reglamento General de Protección de Datos para las instituciones y organismos de la UE[70]. El Comité Europeo de Protección de Datos (CEPD), órgano que agrupa a las Autoridades de Protección de datos de la UE y al Supervisor Europeo de Protección de Datos (SEPD), aprobó en 2021 una guía sobre las limitaciones al derecho de protección de datos conforme al artículo 23 RGPD[71].

En el caso del Consejo de Europa, la cláusula de limitación general del artículo 8 (2) CEDH se concreta en el artículo 11 del Convenio STCE 108+; y más recientemente se han incorporado disposiciones específicas sobre las limitaciones del derecho de protección de datos en el 2.º Protocolo Adicional del Convenio sobre Ciberdelincuencia (Convenio de Budapest)[72]. El Comité Consultivo del Convenio 108, publicó en 2018 una guía práctica sobre el uso de datos personales en el ámbito policial con base en la jurisprudencia del TEDH[73].

---

68 RGPD, artículo 23 (1) d.

69 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo; ELI: http://data.europa.eu/eli/dir/2016/680/2016-05-04; artículos 13 (3) y 15.

70 Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (Texto pertinente a efectos del EEE). ELI: http://data.europa.eu/eli/reg/2018/1725/oj; artículos 79 (3) y 81.

71 Unión Europea, Comité Europeo de Protección de Datos; «Guidelines 10/2020 on restrictions under Article 23 GDPR», 13 de octubre de 2021.

72 Consejo de Europa, 2.º protocolo adicional al Convenio sobre ciberdelincuencia sobre refuerzo de la cooperación e intercambio de pruebas electrónicas, adoptado por el Consejo de Ministros del Consejo de Europa el 17 de noviembre de 2021, artículo 14.

73 Consejo de Europa, Comité Consultivo del Convenio 108: *Practical guide on the use of personal data in the police sector*; T-PD(2018)01.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

A pesar de que el marco legislativo europeo parece robusto, al menos en lo referido a las condiciones de transparencia de la vigilancia ejercitada por autoridades policiales y judiciales en el marco de la lucha contra la criminalidad, las garantías del principio de transparencia se diluyen en el ámbito de la vigilancia realizada por los servicios de inteligencia en interés de la seguridad nacional. Tradicionalmente, esta tensión entre el principio general de transparencia y las necesidades de opacidad (secreto) en las actividades de los servicios de inteligencia han derivado en marcos legales caracterizados por su complejidad y por la falta de concreción de mecanismos legales de facilitación del derecho de acceso de los interesados a la información[74]. De este modo se provoca la clásica paradoja[75] en la que los organismos que tienen mandato [constitucional] de la defensa del EdD[76] pueden ponerlo en peligro por la ausencia de límites claros en su operativa y de mecanismos adecuados de supervisión[77].

La opacidad tiene como primer frente la pugna con el principio de legalidad, que también es parte integral del EdD. Dicho principio implica la existencia de una seguridad jurídica de modo que las leyes se formulen con la precisión y claridad suficientes para permitir a los sujetos de derecho regular su conducta conforme a las mismas, lo cual resulta esencial para la legislación penal (por aplicación del principio *nullum crimen/nulla poena sine lege*).

Fuera del ámbito penal, y en lo relativo a la regulación de las medidas de vigilancia dirigidas a la protección de la seguridad nacional, el TEDH[78] ha afirmado que la previsibilidad en el contexto especial de las medidas secretas de vigilancia, como la interceptación de las comunicaciones, no puede significar que un individuo deba ser capaz de prever cuándo es probable que las autoridades intercepten sus comunicaciones para que pueda adaptar su conducta en consecuencia. Sin embargo, especialmente cuando un poder conferido al ejecutivo se ejerce en secreto, los riesgos de arbitrariedad son evidentes y, por lo tanto, es esencial contar con normas claras y

74 Un reciente ejemplo lo podemos encontrar en el informe de fecha 11 de octubre de 2022 del Consejo de Transparencia y Buen Gobierno sobre el anteproyecto de Ley de Información Clasificada.

75 Juvenal, *Sátiras*, Sátira VI, «Quis custodiet ipsos custodes?».

76 V. g. Artículo 1 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

77 En la STEDH (Gran Sala) asunto Klass y otros c. Alemania, n.º 5029/71 de 6 de septiembre de 1978, ECLI:CE:ECHR:1978:0906JUD000502971, apartado 49, el Tribunal advertía que los Estados contratantes no disponen de una discreción ilimitada para subordinar con las medidas de vigilancia secreta a las personas sometidas a su jurisdicción. Consciente del peligro, inherente en tal ley, de destruir la democracia con el motivo de defenderla, el Tribunal afirma que los Estados parte no debería adoptar, bajo el pretexto de la lucha contra el espionaje o el terrorismo, cualesquiera medidas que ellos consideren apropiadas.

78 STEDH en el asunto Weber y Sravia c. Alemania, n.º 54934/00, de 29 de junio de 2006, ECLI:CE:ECHR:2006:0629DEC005493400, apartados 93 y 94.

detalladas sobre la interceptación de comunicaciones, sobre todo porque la tecnología disponible para su uso es cada vez más sofisticada. El derecho interno debe ser lo suficientemente claro en sus términos para dar a los ciudadanos una indicación adecuada de las circunstancias y las condiciones en las que las autoridades están facultadas para recurrir a tales medidas.

Además, dado que la aplicación en la práctica de medidas de vigilancia secreta de las comunicaciones no está abierta al escrutinio de los individuos público en general, sería contrario al EdD que la discreción legal otorgada al ejecutivo o a un juez se exprese en términos de un poder ilimitado. En consecuencia, la ley debe indicar el alcance de la discrecionalidad conferida a las autoridades competentes y la forma de su ejercicio con la suficiente claridad para dar al individuo una protección adecuada contra la interferencia arbitraria.

El TEDH también se ha pronunciado con claridad sobre la necesidad de que los afectados por una medida de vigilancia secreta sean informados. El hecho de que las personas afectadas por las medidas de vigilancia secreta no sean notificadas posteriormente una vez que la vigilancia ha cesado no puede justificar por sí mismo la conclusión de que la injerencia no era «necesaria en una sociedad democrática» ya que es la propia ausencia de conocimiento de la vigilancia la que garantiza la eficacia de la injerencia. Sin embargo, tan pronto como pueda realizarse la notificación sin poner en peligro la finalidad de la restricción tras el cese de la medida de vigilancia, deberá facilitarse información a las personas afectadas[79]. El TEDH concluyó que la efectividad del derecho a un recurso efectivo puede verse mermada ante la ausencia de una obligación de informar al sujeto o de una posibilidad real de solicitar y obtener información sobre intercepciones de las autoridades[80]. La notificación a los interesados reviste peculiaridades cuando se emplean métodos de vigilancia estratégica (vigilancia no específica), tal y como se verá en el apartado dedicado a esta modalidad.

Un informe de la Agencia de Derechos Fundamentales de la Unión Europea (FRA) reveló que la legislación de los Estados miembros en materia de vigilancia por servicios de inteligencia era mayoritariamente restrictiva en términos de transparencia y de acceso a la información por los interesados[81]. Al tiempo de dicho informe no existía una obligación de información y sobre el derecho de acceso en ocho Estados miembros (República Checa, Irlanda, Letonia, Lituania, Polonia, Eslovaquia, España y el Reino Unido), y el resto se regulaba por ley, pero con restricciones. En un segundo informe del año 2017 la FRA recomendó a los Estados miembros garantizar que los servicios de inteligencia comprueben la legitimidad de la finalidad y la proporcionalidad de los

79 STEDH (Gran Sala), asunto Roman Zhakarov c. Rusia, n.º 47143/06, de 5 de diciembre de 2015, ECLI:CE:ECHR:2015:1204JUD004714306, apartado 287.

80 *Ibid.*, apartado 298.

81 FRA (2015), *Vigilancia por los servicios de inteligencia: garantías de los derechos fundamentales y recursos en la Unión Europea* (vol. I), 3.1.. Surveillance by intelligence services - Volume I: Member States' legal frameworks, 3.1

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

tratamientos de datos personales antes de limitar el acceso a la información sobre la base jurídica de la excepción de «seguridad nacional». Una autoridad competente debería poder examinar el nivel de confidencialidad, aunque, de forma alternativa, la FRA recomendó que los órganos de supervisión lleven a cabo controles en nombre de los interesados cuando no sea posible realizar la notificación o la divulgación de las medidas de vigilancia[82]. También recomendó que los organismos de supervisión externa de las medidas de vigilancia estén igualmente sujetos al escrutinio público mediante la publicación de informes periódicos de su actividad[83].

3. Garantía de la protección de datos frente a la vigilancia por una autoridad de control independiente

La lista de control del EdD incluye la existencia de una autoridad específica e independiente que garantice el cumplimiento de las condiciones legales de la legislación nacional para hacer efectivos los principios y requisitos internacionales en materia de protección de las personas y de los datos personales[84].

El cumplimiento de los derechos y principios relativos a la protección de datos personales se garantiza mediante la existencia de una autoridad de control independiente. En el caso de la UE, esta garantía reviste carácter esencial e integral, al venir incorporada en el derecho originario de la Unión en el párrafo tercero del artículo 8 CDFUE y en el párrafo segundo del artículo 16 TFUE.

El TJUE ha subrayado la necesidad de su existencia en el asunto *Schrems I* al afirmar que «la garantía de independencia de las autoridades nacionales de control pretende asegurar un control eficaz y fiable del respeto de la normativa en materia de protección de las personas físicas frente al tratamiento de datos personales y debe interpretarse a la luz de dicho objetivo. Esa garantía se ha establecido para reforzar la protección de las personas y de los organismos afectados por las decisiones de dichas autoridades. La creación en los Estados miembros de autoridades de control independientes constituye, pues, un elemento esencial de la protección de las personas frente al tratamiento de datos personales»[85].

82 FRA (2017), *La vigilancia por parte de los servicios de inteligencia: salvaguardias y tutela de los derechos fundamentales en la Unión Europea* - Volumen II, dictamen 14. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update.

83 *Ibid.*, dictamen 5.

84 Consejo de Europa, Comisión de Venecia, «Rule of law checklist» aprobada por el pleno de 11-12 de marzo de 2016; CDL-AD(2016)007rev, apartado F.2.a.iii.

85 TJUE, C-362/14, Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015, Maximillian Schrems contra Data Protection Commissioner, ECLI:EU:C:2015:650, apartado 41.

Si la independencia judicial se ha convertido en uno de los ejes definidores del EdD en la Unión Europea[86], la independencia de las autoridades de control de protección de datos también ha sido objeto de jurisprudencia del TJUE:

— La expresión común usada por el RGPD y por el Convenio STCE n.º 108+ es que dichas autoridades actúan «con total independencia». En el asunto Comisión contra República Federal de Alemania, el TJUE interpretó dicha expresión a la luz del anterior Reglamento de protección de datos de instituciones de la UE, que disponía (como hoy hacen tanto el RPGD como el RGPDUE) que la autoridad de control (en ese caso el SEPD) no puede solicitar ni recibir instrucciones de nadie, ni estar sometida a influencia directa o indirecta[87].

— La independencia total también se predica respecto de la organización interna de la autoridad de control, tal y como se puso de manifiesto en el asunto Comisión contra la República de Austria, en el que se hacía evidente la existencia de un riesgo de parcialidad cuando el personal de la autoridad estaba integrado jerárquicamente en el Ejecutivo, o cuando existía un derecho por parte del Ejecutivo de obtener información sobre la gestión de la autoridad de control[88]. Hoy dicha garantía reforzada sobre autonomía organizativa respecto del personal se recoge explícitamente en el artículo 52 (5) RGPD y de modo implícito el artículo 15 (5) del Convenio STCE n.º 108+[89].

A pesar de la existencia de esta garantía legal y jurisprudencial de independencia, tras la entrada en vigor del RGPD se siguen proyectando sombras sobre la independencia de los supervisores nacionales[90] y europeos[91].

---

86 *Vid.* capítulo V de mi estudio «Derechos fundamentales y Estado de derecho en la Unión Europea», Boletín del Ministerio de Justicia, año LXXV, marzo 2021, núm. 2.238 y Fernando Pablo, M. «Las guerras de la independencia: La renovación de los órganos directivos de la Agencia Española de Protección del Datos y el arte de la larga cambiada», *Diario del Derecho, Estudios y Comentarios*, 18/01/2022(RI§1218792).

87 TJUE, C-518/07, Sentencia del Tribunal de Justicia (Gran Sala) de 9 de marzo de 2010. Comisión Europea contra República Federal de Alemania, ECLI:EU:C:2010:125, apartados 26 a 30.

88 TJUE, C-614/10, Sentencia del Tribunal de Justicia (Gran Sala) de 16 de octubre de 2012. Comisión Europea contra República de Austria, ECLI:EU:C:2012:631, apartados 61 a 66.

89 Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 129.

90 CEPD, 6 de abril de 2022, «Carta sobre los proyectos de legislación nacional que afecta a la Autoridad Supervisora belga» y Tribunal Supremo de España, sala 3.ª, auto de suspensión cautelar del acuerdo del Consejo de ministros de 22 de febrero de 2022, por el que se comunica al Congreso de los Diputados la propuesta de candidatos a ocupar la Presidencia y la Adjuntía de la AEPD a los efectos del artículo 48 de la LOPDATS 3787/2022 - ECLI:ES:TS:2022:3787A.

91 SEPD, nota de prensa de 22 de septiembre de 2022; EDPS takes legal action as new Europol Regulation puts rule of law and EDPS independence.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

Además de estos aspectos estatutarios de la independencia de la autoridad de control definidos por el TJUE, e incorporados por el legislador de la Unión, existe otra vertiente, la de la independencia de recursos humanos, técnicos y financieros, así como de locales e infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, que está siendo puesto en duda por las propias autoridades de control en los informes periódicos publicados por el CEPD[92].

En su informe sobre los servicios de inteligencia, la Agencia de Derechos Fundamentales de la UE (FRA) ha concluido que en la mayoría de los Estados miembros las autoridades de supervisión de datos personales carecen de competencia sobre la actividad de los servicios de inteligencia, o sus poderes están muy limitados. Únicamente en Austria, Bulgaria, Croacia, Eslovenia, Finlandia, Hungría y Suecia las autoridades de protección de datos extienden sus competencias sobre la vigilancia ejercitada por los servicios de inteligencia[93].

4. La existencia de vías de recurso frente a la vigilancia

Además de la figura de la autoridad supervisora en el ámbito de la protección de datos personales, una garantía clave frente a la vigilancia ejercida por personas privadas y autoridades es la posibilidad de ejercitar un recurso frente a dicho tratamiento de datos personales. Existe un claro vínculo entre el reconocimiento de un derecho fundamental y la posibilidad real de hacerlo efectivo mediante la tutela reconocida en el art. 1 3 CEDH y 47 CDFUE. Como ya se ha visto con ocasión de las transferencias internacionales de datos, el TJUE puso de manifiesto la esencialidad de este vínculo como motivo para anular las decisiones de adecuación de la Comisión europea en los asuntos *Schrems I y II*.

Desde la perspectiva de la CEDH, el recurso efectivo puede ejercitarse ante una instancia nacional, aunque no tenga carácter judicial (esto es, que no se trate de un tribunal en los términos del artículo 6 CEDH).

El RGPD habilita una doble vía de recurso frente a tratamientos que no respeten el derecho a la protección de datos personales: en primer lugar, existe la posibilidad de obtener una tutela presentando una reclamación ante una autoridad de control[94]; pero

92 CEPD, 5 de agosto de 2021 y 5 de septiembre de 2022, «Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities».

93 FRA (2017), *La vigilancia por parte de los servicios de inteligencia: salvaguardias y tutela de los derechos fundamentales en la Unión Europea* - Volumen II. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update, pp. 80 y 81.

94 RGPD, artículo 77.

también el interesado puede acudir directa[95] y subsidiariamente[96] a los tribunales[97]. Este modelo de doble tutela también existe en la Directiva 2016/680 cuando la vigilancia tiene como fin la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales[98].

La mayor dificultad para los interesados en el ejercicio de vías de recurso y de tutela judicial de sus derechos frente a la vigilancia reside en la mayor opacidad de las acciones de vigilancia y de las limitaciones a los derechos de transparencia asociados a la necesidad de evitar la frustración de investigaciones en curso. La posibilidad de revisión de la legalidad de las acciones de vigilancia es intrínseca al control de la legalidad de la prueba cuando el producto de la vigilancia se incorpora al proceso penal.

Sin embargo, la posibilidad real de acceder a la vía de recurso se dificulta cuando la vigilancia se realiza en entornos más opacos, como el de la seguridad nacional, en los que difícilmente el sujeto vigilado tendrá noticia de las medidas adoptadas. El TEDH, en el asunto *Zakharov* dejó claro que el acceso efectivo a las vías de recurso frente a la vigilancia secreta dependía bien de la notificación al interesado, bien de una posibilidad efectiva de solicitar y obtener de las autoridades acceso a la información sobre las intervenciones[99].

Aun en el caso de que exista este acceso a la vía de recurso frente a la vigilancia realizada por organismos de inteligencia, el verdadero problema reside en las dificultades que los tribunales o las autoridades independientes revisoras tienen para acceder a registros, procedimientos y documentos que con frecuencia revisten carácter de secreto nacional. Incluso cuando estas autoridades tienen este acceso, dichas autoridades necesitan con frecuencia la asistencia de expertos independientes que les permitan comprender la naturaleza de la técnica de vigilancia secreta empleada[100].

---

95 RGPD artículo 79.

96 RGPD artículo 78.

97 *Vid.* las conclusiones del Abogado General Sr. J. Richard de la Tour, presentadas el 8 de septiembre de 2022 en el asunto C-132/21 Nemzeti Adatvédelmi és Információszabadság Hatóság, ECLI:EU:C:2022:661.

98 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo; ELI: http://data.europa.eu/eli/dir/2016/680/oj, artículos 52 a 54.

99 STEDH (Gran Sala) de 5 de diciembre de 2015 en el asunto Roman Zakharov c. Rusia n.º 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306; párrafos 287, 289 y 298.

100 FRA (2017), Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU; cap. 14.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

II. Vigilancia específica

La lista de control del EdD define la vigilancia específica como la captación encubierta de conversaciones por medios tecnológicos, la captación encubierta de telecomunicaciones y la captación encubierta de metadatos[101], si bien matiza que la inclusión de este último concepto aún estaba sometido a discusión[102]. El TJUE, en su jurisprudencia relativa a la conservación de datos, ha indicado que, dentro de las distintas categorías de metadatos, los datos de tráfico y de localización pueden revelar información sobre un número considerable de aspectos de la vida privada de las personas de que se trate, incluida información de carácter sensible, como la orientación sexual, las opiniones políticas, las creencias religiosas, filosóficas, sociales u otras y el estado de salud, dado que estos datos gozan, además, de una protección particular en el Derecho de la Unión. Considerados en su conjunto, estos datos pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones y los círculos sociales que frecuentan. En particular, estos datos proporcionan medios para determinar el perfil de las personas afectadas, información tan sensible, a la luz del respeto de la vida privada, como el propio contenido de las comunicaciones[103].

La lista de control también advierte que los desarrollos tecnológicos hacen cada vez más fácil realizar este tipo de vigilancia, resultando crucial que ello no dote al Estado de un control ilimitado sobre la vida de los individuos[104]. Sin embargo, esta referencia orwelliana al Estado policial no debería interpretarse como una limitación de la lista de control a la vigilancia específica ejecutada por las autoridades, ya sea en el ámbito de la lucha contra la criminalidad o en el de la seguridad nacional, porque el propio concepto de Estado de derecho, como se ha indicado anteriormente, también alcanza a la actividad de personas privadas consecuencia de lo que ha venido a denominarse «capitalismo de la vigilancia»[105].

---

101 Consejo de Europa, Lista de control del Estado de derecho de la Comisión de Venecia, CDL-AD(2016)007rev, apartado 119.

102 Consejo de Europa, Lista de control del Estado de derecho de la Comisión de Venecia, CDL-AD(2016)007rev, nota a pie de página 151. La lista de control hace referencia a la jurisprudencia del TJUE y del TEDH, y al informe CDL-AD(2015)006 de la Comisión de Venecia, que concluyó que en caso de que no exista una autorización judicial previa de la captación de metadatos, debe existir al menos una supervisión independiente y fuerte posteriormente.

103 STJUE (Gran Sala) de 6 de octubre de 2020 en los asuntos acumulados La Quadrature du Net y otros, ECLI:EU:C:2020:791, apartado 191.

104 Consejo de Europa, Lista de control del Estado de derecho de la Comisión de Venecia, CDL-AD (2016)007rev, apartado 118.

105 Zuboff, S. (2000). *La era del capitalismo de la vigilancia*. Paidos. La autora define el capitalismo de la vigilancia del siguiente modo: «El capitalismo de la vigilancia reclama unilateralmente para sí la experiencia humana, entendiéndola como una materia prima gratuita que puede tradu-

Un ejemplo del uso de la vigilancia específica por determinadas empresas privadas, con graves repercusiones para el EdD, fue el escándalo de «Facebook-Cambridge Analytica» desvelado en marzo de 2018, y que demostró que la recopilación de datos personales de usuarios de Facebook (y de sus contactos) permite elaborar mediante el «*microtargeting*» perfiles psicológicos, de manera que se hagan más efectivos los mensajes políticos dirigidos a determinados electores (o perfiles de electores) para manipular su conducta en un proceso electoral[106].

La Comisión de Venecia del Consejo de Europa, consciente del potencial lesivo de este tipo de vigilancia, tanto por actores privados como por potencias extranjeras, ha adoptado unos principios sobre un uso respetuoso con los derechos fundamentales de las tecnologías digitales en los procesos electorales[107].

También la UE ha adoptado medidas legislativas encaminadas a reforzar la protección de datos personales en el marco de las Elecciones al Parlamento Europeo[108]. Más recientemente, el propio Parlamento Europeo adoptó una resolución sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación[109] que considera que las injerencias extranjeras constituyen una grave violación de los valores y principios universales en los que se fundamenta la

---

cir en datos de comportamiento. Aunque algunos de dichos datos se utilizan para mejorar productos o servicios, el resto es considerado como un excedente conductual privativo ("propiedad") de las propias empresas capitalistas de la vigilancia y se usa como insumo de procesos avanzados de producción conocidos como inteligencia de máquinas, con los que se fabrican productos predictivos que prevén lo que cualquiera de ustedes hará ahora, en breve y más adelante. Por último, estos productos predictivos son comprados y vendidos en un nuevo tipo de mercado de predicciones de comportamientos que yo denomino mercados de futuros conductuales. Los capitalistas de la vigilancia se han enriquecido inmensamente con esas operaciones comerciales, pues son muchas las empresas ansiosas por apostar sobre nuestro comportamiento futuro».

106 Resolución del Parlamento Europeo, de 25 de octubre de 2018, sobre la utilización de los datos de los usuarios de Facebook por parte de Cambridge Analytica y el impacto en la protección de los datos (2018/2855(RSP), puntos Y y Z. Sobre la técnica de análisis de macrodatos y elaboración de perfiles con fines electorales, véase el informe de la Autoridad de protección de datos del Reino Unido (2018), «Democracy Disrupted?: Personal information and political influence».

107 Comisión de Venecia del Consejo de Europa (2020) Study - Principles for a fundamental rights-compliant use of digital technologies in electoral processes, approved by the Council for Democratic Elections at its 70th meeting (online, 10 December 2020) and adopted by the Venice Commission at its 125th Plenary Session (online, 11-12 December 2020) CDL-AD(2020)037-e.

108 Reglamento (UE, Euratom) 2019/493 del Parlamento Europeo y del Consejo, de 25 de marzo de 2019, por el que se modifica el Reglamento (UE, Euratom) n.º 1141/2014 en lo que respecta a un procedimiento de verificación relativo a las infracciones de las normas de protección de los datos personales en el contexto de las elecciones al Parlamento Europeo, ELI: http://data.europa.eu/eli/reg/2019/493/oj.

109 Parlamento Europeo; Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación (2020/2268(INI)).

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

Unión, como la dignidad humana, la libertad, la igualdad, la solidaridad, el respeto de los derechos humanos y las libertades fundamentales, la democracia y el Estado de derecho[110]. Más concretamente, la resolución considera que las plataformas sociales, los dispositivos y las aplicaciones digitales recaban y almacenan enormes cantidades de datos personales muy detallados y, a menudo, sensibles, sobre cada usuario; que esta información puede utilizarse para predecir tendencias de comportamiento, reforzar sesgos cognitivos y orientar la toma de decisiones; que esta información se explota con fines comerciales; que las fugas de datos se producen repetidamente, en detrimento de la seguridad de las víctimas de dichas fugas, y que los datos pueden venderse en el mercado negro; que tales bases de datos podrían constituir minas de oro para los agentes malintencionados que deseen actuar contra grupos o individuos[111].

Cuando la vigilancia específica se realiza por autoridades en el marco de investigaciones criminales y para la protección de la seguridad nacional, el TEDH ha fijado seis garantías mínimas que debe establecer la ley para evitar el abuso de poder[112].

1.ª La naturaleza de los delitos que pueden dar lugar a una orden de intervención.

2.ª La definición de las categorías de personas susceptibles de estar sujetas a la intervención.

3.ª El límite de duración de la intervención.

4.ª El procedimiento para acceder, usar y conservar la información intervenida.

5.ª Las cautelas a adoptar en caso de comunicación de la información interceptada a terceros.

6.ª Las circunstancias en las que la información interceptada debe ser borrada o destruida.

La lista de control del EdD plantea, de modo algo más simplificado al referirse únicamente a los requisitos de la legislación, cuatro puntos de comprobación sobre las medidas de vigilancia específica[113]:

1.º La existencia de una provisión sobre la medida en la legislación sujeta a principios como el de proporcionalidad.

2.º La existencia de normas que regulen procedimientos de control y supervisión de la medida.

---

110 *Ibid*., considerando A.

111 *Ibid*., considerando AJ.

112 STEDH (Gran Sala) de 5 de diciembre de 2015 en el asunto Roman Zakharov c. Rusia n.º 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, apartados 231, 238 y jurisprudencia citada.

113 Consejo de Europa, Lista de control del Estado de derecho de la Comisión de Venecia, CDL-AD(2016)007rev, apartado F.2.b.

3.º El requisito de la autorización previa de la medida por un juez o por una institución independiente.

4.º La existencia de vías de recurso suficientes frente a posibles vulneraciones de los derechos individuales.

La naturaleza del delito objeto de investigación o prevención resulta especialmente relevante a la hora de configurar las restantes garantías conforme a los principios de necesidad y de proporcionalidad. En el asunto *Ministerio Fiscal* el TJUE adoptó una regla de proporcionalidad entre el nivel de injerencia en los derechos fundamentales a la vida privada y a la protección de datos personales y la gravedad del delito que se pretende prevenir, investigar, descubrir o perseguir[114]: a mayor injerencia de una medida de vigilancia, mayor deberá ser la gravedad del delito. Así, por ejemplo, el acceso por las autoridades, por un tiempo limitado, a los datos de titularidad de una tarjeta SIM activada en un determinado terminal, por sí solo (sin cruzar este dato con otros relativos a las comunicaciones o a la localización del terminal) no permite extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados. Por lo tanto, al no ser una injerencia grave no es preciso que la medida se reserve para actividades de vigilancia de delincuencia grave, sino que puede ser usada para la delincuencia en general[115]. Sin embargo, solo la lucha contra la delincuencia grave puede justificar un acceso a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas que, considerados en su conjunto, permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos han sido conservados[116].

El nivel de intrusión de la vigilancia específica ha alcanzado una gran magnitud con la introducción de herramientas de vigilancia como el «*spyware*»que permiten un control absoluto e indetectable de dispositivos móviles, de manera que, además de la intercepción del contenido y los metadatos de comunicaciones telefónicas o telemáticas, todos los sensores del dispositivo infectado quedan bajo el control del vigilante, de modo que puede activar y usar la información del micrófono, la cámara, el GPS, etc., incluso cuando el terminal no está siendo usado por el sujeto vigilado[117].

Consecuentemente, un mayor nivel de intrusión se refleja en una mayor injerencia en los derechos humanos de los interesados[118]. Sin perjuicio de que la naturaleza de este tipo de medidas de vigilancia está siendo objeto de escrutinio por un comité *ad hoc* del

114 STJUE (Gran Sala) de 2 de octubre de 2018 en el asunto C-207/16 Ministerio Fiscal, ECLI:EU:C:2018:788, apartado 56.

115 *Ibid*., apartados 59 a 63.

116 *Ibid.,* apartado 54.

117 Marzocchi, O. y Mazzini, M. (2022). Pegasus and surveillance spyware. Estudio para el Parlamento Europeo; PE 732.268.

118 Informe del Departamento de Sociedad de la Información del Consejo de Europa «Pegasus Spyware and its impact on human rights»; DGI(2022)04.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

Parlamento Europeo[119], el Supervisor Europeo de Protección de Datos (SEPD), en sus observaciones preliminares, ha indicado que parece poco probable que este tipo de *software* pueda cumplir con el criterio de proporcionalidad porque su intrusividad es tan alta que priva de facto del derecho a la intimidad del sujeto vigilado con afectación al núcleo de este derecho[120] y por ello recomienda que se proceda a aprobar una normativa que prohíba el desarrollo y uso de herramientas similares a Pegasus en la UE[121].

En cuanto al requisito de la supervisión de la vigilancia específica, el TEDH consolidó su doctrina en el asunto *Roman Zakharov c. Rusia*[122], con una división en tres etapas: cuando se ordena la vigilancia por primera vez, mientras se está llevando a cabo y después de que haya terminado.

En las dos primeras etapas, la propia naturaleza y la lógica de la vigilancia secreta dictan que no solo la vigilancia en sí misma, sino también la revisión que la acompaña debe efectuarse sin el conocimiento del individuo. Por lo tanto, dado que el individuo se verá necesariamente impedido de buscar un recurso efectivo por sí mismo o de participar directamente en cualquier procedimiento de revisión, es esencial que los procedimientos establecidos proporcionen por sí mismos garantías adecuadas y equivalentes que salvaguarden sus derechos. Además, los valores de una sociedad democrática deben seguirse tan fielmente como sea posible en los procedimientos de supervisión si no se quieren sobrepasar los límites de la necesidad, en el sentido del artículo 8 (2) CEDH. En un ámbito en el que el abuso es potencialmente tan fácil en los casos individuales y podría tener consecuencias tan perjudiciales para la sociedad democrática en su conjunto, es en principio deseable confiar el control de supervisión a un juez, ya que el control judicial ofrece las mejores garantías de independencia, imparcialidad y un procedimiento adecuado (véase *Klass y otros*, §§ 55-56)[123].

Por lo que respecta a la tercera etapa, una vez finalizada la vigilancia, la cuestión de la notificación posterior de las medidas de vigilancia está inextricablemente ligada a la eficacia de los recursos ante los tribunales y, por tanto, a la existencia de garantías efectivas contra el abuso de los poderes de vigilancia. En principio, hay pocas posibilidades de que el individuo afectado recurra a los tribunales, a menos que se le notifiquen las medidas adoptadas sin su conocimiento y, por lo tanto, pueda impugnar su legalidad *a posteriori* (véase *Klass y otros*, § 57, y *Weber y Saravia*, § 135) o, alternativamente, a menos que cualquier persona que sospeche que sus

119 Parlamento Europeo, Comisión de Investigación Encargada de Examinar el Uso del Programa Espía de Vigilancia Pegasus y Otros Programas Equivalentes.

120 SEPD (2022) Preliminary remarks on modern spyware, p. 8.

121 *Ibid.,* p. 9.

122 STEDH (Gran Sala) de 5 de diciembre de 2015 en el asunto Roman Zakharov c. Rusia n.º 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306.

123 *Ibid.,* apartado 233.

comunicaciones están siendo o han sido interceptadas pueda dirigirse a los tribunales, de modo que la competencia de estos no dependa de la notificación al sujeto de la interceptación de que se han interceptado sus comunicaciones (véase la sentencia Kennedy, § 167)[124].

III. Vigilancia estratégica

La inteligencia de telecomunicaciones (en inglés *signals intelligence*) se define en la lista de control del EdD como los medios y métodos para la interceptación de telecomunicaciones incluyendo las efectuadas por medio de ondas de radio, satélite, teléfono móvil o cable[125]. Tradicionalmente, este tipo de inteligencia pertenecía al ámbito militar, teniendo como objetivo las telecomunicaciones cifradas militares de otros países, pero el desarrollo del Internet y el uso de telecomunicaciones por grupos terroristas (en especial tras el 11-S)[126] extendieron el empleo de la misma doctrina al ámbito de las telecomunicaciones civiles, con el consiguiente aumento de la injerencia en los derechos y libertades de los individuos[127].

El TEDH ha reconocido que, si bien las capacidades tecnológicas han aumentado considerablemente el volumen de las comunicaciones que atraviesan Internet, también han proliferado las amenazas a las que se enfrentan los Estados contratantes y sus ciudadanos. Estas incluyen, entre otras, el terrorismo global, el tráfico de drogas, la trata de personas y la explotación sexual de los niños. Muchas de estas amenazas provienen de redes internacionales de actores hostiles con acceso a una tecnología cada vez más sofisticada que les permite comunicarse sin ser detectados. El acceso a dicha tecnología también permite a actores hostiles estatales y no estatales perturbar la infraestructura digital e incluso el correcto funcionamiento de los procesos democráticos mediante el uso de ciberataques, una grave amenaza para la seguridad nacional que, por definición, solo existe en el ámbito digital y, como tal, solo puede detectarse e investigarse allí[128].

Por vigilancia estratégica[129] se entiende la inteligencia de telecomunicaciones extendida al ámbito civil. Se diferencia de la vigilancia específica en su dimensión y

124 *Ibid.,* apartado 234.

125 Consejo de Europa, Comisión de Venecia, «Rule of law checklist» aprobada por el pleno de 11-12 de marzo de 2016; CDL-AD(2016)007rev, apartado F (2), punto 120.

126 Ruiz Dorado, M. Constitución y espionaje (2022), Ed. Tirant lo Blanch.

127 *Ibid.* Punto 121 y nota a pie de página 156.

128 STEDH (Gran Sala) de 25 de mayo de 2021 en el asunto n.º 35252/08 Centrum för Rättvisa c. Suecia, ECLI:CE:ECHR:2021:0525JUD003525208, apartado 237.

129 El término usado en los textos originales del informe de la Comisión de Venecia (*strategic surveillance/surveillance stratégique*) procede de la legislación alemana (*strategische Beschränkung*). El uso de esta terminología responde a que los primeros casos analizados en el TEDH fueron alemanes (Klasss y otros c. Alemania, n.º 5029/71, y Weber y Saravia c. Alemania, n.º 54934/00).

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

finalidad: la vigilancia estratégica se aplica sobre el conjunto de comunicaciones electromagnéticas (por ejemplo, mediante el análisis de todas las comunicaciones [contenido y metadatos] que atraviesan un cable de fibra óptica submarino intercontinental o las que retransmite un satélite de telecomunicaciones) y su finalidad no es la obtención de pruebas para la prevención, investigación o represión de un delito, sino la recopilación de informaciones relevantes para los fines de la seguridad nacional. Dicho en otras palabras, mientras que la vigilancia específica se aplica cuando ya existen uno o varios sujetos que vigilar por un hecho que motiva esta investigación, la vigilancia estratégica desconoce al sujeto y se orienta a la extracción de informaciones (sobre el conjunto de comunicaciones) que pueden resultar útiles a los fines de la seguridad nacional (v. g. la existencia de un riesgo desconocido)[130].

El TEDH considera que la vigilancia estratégica es un proceso gradual en el que el nivel de interferencia con los derechos del artículo 8 de los individuos aumenta a medida que el proceso avanza. Es posible que no todos los regímenes de vigilancia estratégica sigan exactamente el mismo modelo, y que las diferentes etapas del proceso no sean necesariamente discretas ni se sigan en estricto orden cronológico. No obstante, el Tribunal considera que las etapas del proceso pueden describirse del siguiente modo:

(a) la interceptación y retención inicial de las comunicaciones y de los datos de las comunicaciones relacionadas (es decir, los datos de tráfico pertenecientes a las comunicaciones interceptadas)[131];

(b) la aplicación de selectores específicos a las comunicaciones y datos de comunicaciones relacionados retenidos[132];

130 Comisión de Venecia del Consejo de Europa, Informe sobre la supervisión democrática de las agencias de intercepción de telecomunicaciones, 21 de marzo de 2015, CDL-AD(2015)011, apartado 47.

131 Esta interceptación puede realizarse de modo directo por las autoridades (v. g. interceptando el tráfico de datos de un cable de fibra óptica intercontinental) o de modo indirecto, imponiendo una obligación de conservación o de transmisión de datos a los proveedores de servicios, si bien esta conservación puede ser útil tanto a los efectos de la vigilancia estratégica como a los de la vigilancia específica (siempre que se dispongan de datos suficientes sobre el objetivo).

132 Dado el volumen, variedad y velocidad de los datos capturados, el único modo de realizar la vigilancia estratégica es mediante el uso de la inteligencia artificial, que permite «encontrar la aguja en el pajar» mediante la definición previa de una serie de selectores/discriminadores algorítmicos (por ejemplo, el idioma usado, la procedencia o el destino de la comunicación, el uso de un determinado patrón en el procesamiento automatizado del lenguaje natural, el uso de un tipo particular de cifrado...etc.) que de modo combinado permiten realizar una búsqueda automatizada en el flujo de información, cuyo producto será posteriormente objeto del trabajo de analistas de inteligencia, con diseminación del material relevante a los servicios operativos. Una descripción del sistema técnico (llamado en inglés *Bulk collection of signals intelligence*) se encuentra en el modelo conceptual del informe sobre opciones técnicas del Comité académico de EE. UU. en relación a la directiva presidencial 28 - Committee on Responding to Section 5(d) of Presidential Policy Directive 28: The Feasibility of Software to Provide Alternatives to Bulk Signals Intelligence Collection. Otra fuente descriptiva del uso de vigilancia estratégica se hizo pública en octubre de

(c) el examen de los datos de comunicaciones/comunicaciones relacionadas seleccionados por parte de los analistas; y

(d) la posterior conservación de los datos y el uso del «producto final», incluida la puesta en común de los datos con terceros[133].

La lista de control del EdD de la Comisión de Venecia propone una serie de medidas legislativas como garantías de prevención frente al abuso de la vigilancia estratégica[134]:

1.ª La existencia de normativa que regule los principales elementos de la vigilancia estratégica, incluyendo la definición de las agencias autorizadas a realizarla, las concretas finalidades de esta y sus límites, incluyendo el principio de proporcionalidad en la recolección, conservación y diseminación de los datos.

2.ª Que la normativa reguladora de la privacidad y de la protección de datos ampare los derechos de extranjeros o no residentes.

3.ª Que la vigilancia estratégica esté sometida a autorización previa por un juez o por una autoridad administrativa independiente y que existan mecanismos de supervisión y control independientes.

4.ª La existencia de recursos efectivos frente al posible uso de la vigilancia estratégica.

Debido a la especial naturaleza de la vigilancia estratégica, el TEDH decidió actualizar las garantías prevenidas en su jurisprudencia aplicable a la vigilancia específica[135] en el asunto *Big Brother Watch y otros c. Reino Unido.* El Tribunal dejó claro que la garantía relativa a la naturaleza del delito o las categorías de personas susceptibles de ser vigiladas no son fácilmente aplicables a la vigilancia estratégica. Por el mismo motivo, tampoco sería pertinente la exigencia de una sospecha razonable, al tener la vigilancia estratégica una finalidad preventiva. No obstante, el Tribunal considera imperativo que, cuando un Estado aplique un régimen de este tipo, el Derecho interno contenga normas detalladas sobre cuándo pueden las autoridades recurrir a tales medidas. En particular, el Derecho interno debe establecer con suficiente claridad los motivos por los que se puede autorizar la vigilancia estratégica y las circunstancias en las que se pueden interceptar las comunicaciones de una persona. Las cuatro garantías mínimas restantes definidas por el Tribunal en sus sentencias anteriores —es decir, que el

---

2016 por los servicios de inteligencia de los Países Bajos: https://open.overheid.nl/repository/ronl-4fc445cdbbbe1093715d25ac58eed8960e08ff54/1/pdf/Visual%20Waarborgen%20onderzoeksopdrachtgerichte%20interceptie.pdf. Véase también STEDH (Gran Sala) de 25 de mayo de 2021 en el asunto n.º 35252/08 Centrum för Rättvisa c. Suecia, apartado 306.

133 STEDH (Gran Sala) de 25 de mayo de 2021 en el asunto n.º 35252/08 Centrum för Rättvisa c. Suecia, ECLI:CE:ECHR:2021:0525JUD003525208, apartado 239.

134 Consejo de Europa, Lista de control del Estado de derecho de la Comisión de Venecia, CDL-AD(2016)007rev, apartado 119.

135 Véanse las seis garantías reseñadas en el capítulo anterior.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

derecho interno debe establecer un límite a la duración de la interceptación, el procedimiento que debe seguirse para examinar, utilizar y almacenar los datos obtenidos, las precauciones que deben tomarse al comunicar los datos a terceros y las circunstancias en las que los datos interceptados pueden o deben ser borrados o destruidos— son igualmente pertinentes para la vigilancia estratégica[136].

Por otro lado, en el contexto de la vigilancia estratégica, la importancia de la supervisión y la revisión se amplía, debido al riesgo inherente de abuso y a que la necesidad legítima de mantener el secreto significará inevitablemente que, por razones de seguridad nacional, los Estados a menudo no tendrán la libertad de revelar información relativa al funcionamiento del régimen impugnado[137]. Por lo tanto, para minimizar el riesgo de que se abuse de la vigilancia estratégica, el Tribunal considera que el proceso debe estar sujeto a «salvaguardias de extremo a extremo», lo que significa que, a nivel nacional, debe realizarse una evaluación en cada fase del proceso sobre la necesidad y la proporcionalidad de las medidas que se adopten; que la vigilancia estratégica debe estar sujeta a una autorización independiente al principio, cuando se definan el objeto y el alcance de la operación; y que la operación debe estar sujeta a supervisión y a una revisión independiente *a posteriori*. En opinión del Tribunal, se trata de salvaguardias fundamentales que constituirán la piedra angular de cualquier régimen de vigilancia estratégica que se ajuste al artículo 8 CEDH[138].

El TEDH fija el criterio relativo a la autorización previa de la vigilancia estratégica en el sentido de que, si bien la autorización judicial es una importante salvaguarda contra la arbitrariedad, no es un requisito necesario. No obstante, la interceptación en masa debe ser autorizada al menos por un órgano independiente del ejecutivo[139]. Con el fin de proporcionar una salvaguardia eficaz contra los abusos, el organismo autorizador independiente debe ser informado tanto del propósito de la interceptación como de los portadores o las rutas de comunicación que probablemente se intercepten. Esto permitiría al organismo autorizador independiente evaluar la necesidad y la proporcionalidad de la operación de vigilancia estratégica y también evaluar si la selección de los portadores es necesaria y proporcionada a los fines para los que se realiza la interceptación[140].

Teniendo en cuenta las características de la vigilancia estratégica, el gran número de selectores empleados y la necesidad inherente de flexibilidad en la elección de estos, que en la práctica pueden expresarse como combinaciones técnicas de números o letras, el TEDH ha reconocido que la inclusión de todos los selectores en la autorización

136 STEDH de 25 de mayo de 2021 en los asuntos acumulados Big Brother Watch y otros c. Reino Unido, apartado 348.

137 *Ibid.,* apartado 349.

138 *Ibid.,* apartado 350.

139 *Ibid.,* apartado 351.

140 *Ibid.,* apartado 352.

puede no ser factible en la práctica. No obstante, dado que la elección de los selectores y de los términos de consulta determina qué comunicaciones podrán ser examinadas por un analista, la autorización debería, como mínimo, identificar los tipos o categorías de selectores que se utilizarán[141]. Además, deben establecerse mayores garantías cuando los servicios de inteligencia empleen selectores «fuertes» vinculados a personas identificables. El uso de cada uno de estos selectores debe ser justificado por los servicios de inteligencia —con respeto a los principios de necesidad y proporcionalidad—, y dicha justificación debe quedar escrupulosamente registrada y estar sujeta a un proceso de autorización interna previa que prevea la verificación separada y objetiva de la justificación de la medida conforme a dichos principios[142]. Para que esta garantía sea efectiva, el organismo supervisor debe estar en condiciones de evaluar la necesidad y la proporcionalidad de la medida que se adopte, teniendo debidamente en cuenta el correspondiente nivel de intrusión en los derechos del CEDH de las personas que puedan verse afectadas. Para facilitar esta supervisión, los servicios de inteligencia deben llevar un registro detallado de cada etapa del proceso[143].

En relación con las garantías relativas a la existencia de un recurso efectivo, el TEDH considera que un recurso que no dependa de la notificación al sujeto de la interceptación también podría ser un recurso efectivo en el contexto de la vigilancia estratégica; de hecho, dependiendo de las circunstancias, podría incluso ofrecer mejores garantías de un procedimiento adecuado que un sistema basado en la notificación. Independientemente de que el material se haya adquirido mediante la vigilancia específica o estratégica, la existencia de una excepción de seguridad nacional podría privar a un requisito de notificación de cualquier efecto práctico real. La probabilidad de que un requisito de notificación tenga poco o ningún efecto práctico será aún más alta en el contexto de vigilancia estratégica, ya que dicha vigilancia puede utilizarse con fines de recopilación de inteligencia extranjera y, en su mayor parte, se dirigirá a las comunicaciones de personas fuera de la jurisdicción territorial del Estado. Por lo tanto, aunque se conozca la identidad de un objetivo, las autoridades pueden desconocer su ubicación[144].

Las facultades y las garantías procesales que posee una autoridad son relevantes para determinar si un recurso es efectivo. Por lo tanto, en ausencia de un requisito de notificación, es imperativo que el recurso se presente ante un organismo que, aunque no necesariamente sea judicial, sea independiente del ejecutivo y garantice la equidad del procedimiento, ofreciendo, en la medida de lo posible, un proceso contradictorio. Las decisiones de dicha autoridad deberán estar motivadas y ser jurídicamente

141 *Ibid.,* apartado 354.

142 *Ibid.,* apartado 355.

143 *Ibid.,* apartado 356 y STEDH (Gran Sala) de 25 de mayo de 2021 en el asunto n.º 35252/08 Centrum för Rättvisa c. Suecia, apartado 309.

144 *Ibid.,* apartado 358.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

vinculantes en lo que respecta, entre otras cosas, al cese de la interceptación ilegal y a la destrucción del material de interceptación obtenido o almacenado ilegalmente[145].

Si bien tanto la lista de control del EdD como la jurisprudencia del TEDH parecen abordar la vigilancia estratégica bajo el presupuesto de una interceptación de las comunicaciones realizadas directamente por las autoridades, también es posible incluir dentro de este ámbito la vigilancia que se realiza sobre la información que conservan o transmiten[146] a las autoridades los operadores privados de servicios de telecomunicaciones en virtud de una obligación legal. La discusión sobre el alcance de esta obligación ha ido aumentando desde la invalidación por el TJUE de la Directiva 2006/24/CE de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones[147] en el asunto *Digital Rights Ireland Ltd*[148]. Desde dicha invalidación los Gobiernos europeos se han resistido a modificar su legislación de conservación de datos en trasposición de la Directiva anulada, a pesar de las reiteradas ocasiones en las que el TJUE ha subrayado que el mero hecho de la existencia de una conservación general e indiferenciada de los datos de tráfico y localización de los usuarios es una injerencia distinta y adicional a la que se realiza con el acceso posterior por las autoridades a dichos datos conservados: el TJUE considera que la Directiva 2002/58 (Directiva de privacidad de las comunicaciones electrónicas) no se limita a regular el acceso a tales datos mediante garantías dirigidas a prevenir los abusos, sino que también consagra, en particular, el principio de prohibición de su almacenamiento por terceros[149], siendo irrelevante que la información relativa a la vida privada de que se trate tenga o no carácter sensible, que los

145 *Ibid.,* apartado 359. En la STEDH (Gran Sala) de 25 de mayo de 2021 en el asunto n.º 35252/08 Centrum för Rättvisa c. Suecia, apartado 361, añade un requisito de publicidad de los razonamientos.

146 La STJUE (Gran Sala) de 6 de octubre de 2020 en el asunto C-623/17 Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, ECLI:EU:C:2020:790, equipara, en sus apartados 40 y 41, la transmisión y la conservación de los datos por parte de los proveedores de servicios.

147 Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, ELI: http://data.europa.eu/eli/dir/2006/24/oj.

148 STJUE (Gran Sala) de 8 de abril de 2014 en los asuntos acumulados C-293/12 y C-594/12 Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros; ECLI:EU:C:2014:238. Peticiones de decisión prejudicial planteadas por la High Court (Irlanda) y el Verfassungsgerichtshof.

149 STJUE (Gran Sala) de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 39.

interesados hayan sufrido o no inconvenientes en razón de tal injerencia, o si los datos conservados serán o no utilizados posteriormente[150].

La finalidad de la conservación o transmisión de datos por los proveedores de servicios ha sido un elemento clave a la hora de evaluar el alcance de dicha conservación, y en el asunto La Quadrature du Net y otros el TJUE validó que la medida de conservación fuera general e indiferenciada, siempre que existan circunstancias suficientemente concretas que permitan considerar que el Estado miembro en cuestión se enfrenta a una amenaza grave [...] para la seguridad nacional que resulte real y actual o previsible[151]. Esta conservación general e indiferenciada se limitará temporalmente a lo estrictamente necesario, aunque el requerimiento de conservación a los proveedores de servicios pueda eventualmente renovarse también por un tiempo limitado[152]. Con ello el TJUE pretende evitar que la conservación general sea sistemática, evitando que la excepción se convierta en la regla. Además, el TJUE impone que el requisito de conservación general pueda ser objeto de un control efectivo, bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, cuya decisión tenga carácter vinculante, que tenga por objeto comprobar la existencia de una de estas situaciones, así como el respeto de las condiciones y de las garantías que deben establecerse[153].

Debido a la preponderancia de los objetivos relacionados con amenazas reales y graves a la seguridad nacional sobre los relativos a lucha contra la delincuencia grave, el TJUE concluye que una normativa nacional que establece la conservación generalizada e indiferenciada de los datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave excede de los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática[154].

Los criterios relativos a la vigilancia estratégica fijados por el TEDH no resultan directamente aplicables a medidas de conservación sobre el tráfico de datos *ad intra* (esto es, a telecomunicaciones nacionales) y cuando la finalidad de este tratamiento no es la protección de la seguridad nacional, sino la prevención, detección e investigación de delitos graves. Además, el TJUE recuerda que «el artículo 52, apartado 3 CDFUE tiene por objeto garantizar la coherencia necesaria entre los derechos contenidos en ella y los correspondientes derechos garantizados por el CEDH, sin perjuicio de la autonomía del Derecho de la Unión y del Tribunal de Justicia de la Unión Europea, de modo que solo deben tenerse en cuenta los correspondientes derechos

150 *Ibid.*, apartado 44.

151 STJUE (Gran Sala) de 6 de octubre de 2020 en los asuntos acumulados La Quadrature du Net y otros contra Premier ministre y otros; ECLI:EU:C:2020:791; apartado 137.

152 *Ibid.,* apartado 138.

153 *Ibid.,* apartado 139.

154 *Ibid.,* apartados 135,136 y 141.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

del CEDH en vista de la interpretación de la Carta, como umbral de protección mínima»[155].

Debido a esta autonomía, el TJUE ha fijado su propio marco de garantías en la conservación selectiva de los datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave y de la prevención de las amenazas graves a la seguridad pública, así como a efectos de la protección de la seguridad nacional, siempre que dicha conservación de los datos esté limitada a lo estrictamente necesario en relación con las categorías de datos que deban conservarse, los medios de comunicación a que se refieran, las personas afectadas y el período de conservación establecido[156].

El criterio personal de especificación de la medida de conservación selectiva puede tener como objetivo aquellas personas que se han identificado previamente, en el marco de procedimientos nacionales aplicables y sobre la base de elementos objetivos, como una amenaza para la seguridad pública o la seguridad nacional del Estado miembro en cuestión[157]. Los criterios objetivos para evaluar la necesidad y proporcionalidad de una medida de conservación selectiva sobre determinadas personas pueden variar en función de las medidas adoptadas a efectos de la prevención, la investigación, el descubrimiento y la persecución de la delincuencia grave; dichas personas pueden, en particular, ser aquellas que han sido identificadas previamente, en el marco de procedimientos nacionales aplicables y sobre la base de elementos objetivos y no discriminatorios, como una amenaza para la seguridad pública o la seguridad nacional del Estado miembro en cuestión[158]. De esta manera, los Estados miembros tienen la facultad de adoptar medidas de conservación sobre personas a las que se identifica porque están siendo investigadas o, están siendo objeto de otras medidas de vigilancia o constan en el registro nacional de antecedentes penales por una condena anterior por delitos graves que pueden implicar un elevado riesgo de reincidencia[159].

Esta cuestión resulta de extraordinaria importancia a la hora de analizar la posible incorporación de datos de vigilancia específica como prueba en un proceso penal, aun cuando el origen de dicha información (identificación subjetiva o atribución) haya sido producto de la vigilancia estratégica por motivos de seguridad nacional. De ello se sigue igualmente que la circunstancia de que los datos de tráfico y los datos de localización hayan sido legalmente objeto de conservación a efectos de la protección de la seguridad nacional no afecta a la licitud de su conservación con fines de lucha

155 STJUE (Gran Sala) de 20 de septiembre de 2022 en los asuntos acumulados C-793/19 y C-794/19 SpaceNet AG y Telekom Deutschland GmbH; ECLI:EU:C:2022:702; apartado 125.

156 *Ibid.,* apartado 147.

157 *Ibid.,* apartado 149.

158 STJUE (Gran Sala) de 5 de abril de 2022 en el asunto C-140/20 G.D. contra Commissioner of the Garda Síochána y otros, ECLI:EU:C:2022:258, apartado 77.

159 *Ibid.,* apartado 78.

contra la delincuencia grave[160]. Sin embargo, el TJUE ha descartado que las autoridades puedan acceder directamente a datos conservados de modo general e indiferenciado bajo la normativa reguladora de la seguridad nacional con el fin de luchar contra la delincuencia grave, ya que sería contrario a la jerarquía de objetivos de interés general. Si estos datos han sido excepcionalmente conservados de manera generalizada e indiferenciada, con fines de protección de la seguridad nacional contra una amenaza que resulta real y actual o previsible, las autoridades nacionales competentes en materia de investigación de los delitos no pueden acceder a dichos datos en el marco de un proceso penal, so pena de privar de todo efecto útil a la prohibición de efectuar tal conservación a efectos de la lucha contra la delincuencia grave[161].

En segundo lugar, la conservación selectiva puede basarse asimismo en un criterio geográfico cuando las autoridades nacionales competentes consideren, sobre la base de elementos objetivos y no discriminatorios, que existe una situación caracterizada por un riesgo elevado de preparación o de comisión de tales delitos graves en una o varias zonas geográficas. Estas zonas pueden ser, en particular, lugares que cuentan con un número elevado de delitos graves, lugares especialmente expuestos a la comisión de delitos graves, como los lugares o infraestructuras a los que acuden con regularidad un número muy elevado de personas, o incluso lugares estratégicos, como aeropuertos, estaciones o zonas de peajes[162]. En la medida en que una conservación selectiva fundada en tal criterio puede afectar, en función de los delitos graves contemplados y de la situación específica de los Estados miembros respectivos, tanto a lugares en los que se produce un elevado número de delitos graves como a los lugares especialmente expuestos a la comisión de tales delitos, en principio, tampoco puede dar lugar a discriminaciones, pues el criterio relativo a la tasa media de delincuencia grave no presenta, en sí mismo, ningún vínculo con elementos potencialmente discriminatorios[163].

En cuanto a la posibilidad de establecer algún criterio distintivo que no sea ni personal ni geográfico para efectuar una conservación selectiva de datos de tráfico y de localización, no puede excluirse que se tengan en cuenta otros criterios, objetivos y no discriminatorios, para garantizar que el alcance de una conservación selectiva se limite a lo estrictamente necesario y establecer un vínculo, al menos indirecto, entre los delitos graves y las personas cuyos datos va a conservarse[164]. En cualquier caso, la eventual existencia de dificultades para definir con precisión los casos y las condiciones en que pueda realizarse una conservación selectiva no justifica que los Estados

160 *Ibid.* apartado 64.

161 STJUE (Gran Sala) de 5 de abril de 2022 en el asunto C-140/20 G.D. contra Commissioner of the Garda Síochána y otros, ECLI:EU:C:2022:258, apartados 96 a 100.

162 *Ibid.,* apartado 150.

163 *Ibid.,* apartado 80.

164 *Ibid.,* apartado 83.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

miembros, haciendo de la excepción una norma, establezcan una conservación generalizada e indiferenciada de datos de tráfico y de localización[165].

En relación con la fase de análisis automatizado (el filtrado) de los datos de tráfico y de localización previamente conservados, el TJUE dispone que la autoridad nacional competente tiene la obligación de publicar información de carácter general relativa a dicho análisis, sin tener que informar individualmente a las personas afectadas. En cambio, en el supuesto de que los datos respondan a los parámetros precisos en la medida en que autorizan el análisis automatizado o de que dicha autoridad proceda a identificar a la persona afectada para analizar más en profundidad los datos que la conciernen, la información individual de esta persona resulta necesaria. No obstante, únicamente debe procederse a esa información siempre que y a partir del momento en que no pueda comprometer las misiones que corresponden a dicha autoridad[166]. El análisis automatizado debe poder ser objeto de un control efectivo, bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, cuya decisión tenga carácter vinculante, que tenga por objeto comprobar la existencia de una situación que justifique dicha medida, así como el respecto de las condiciones y de las garantías que deben establecerse[167].

IV Videovigilancia

Tal y como se indicaba en la introducción de este estudio, el sentido predominante en los homínidos es la vista, de ahí que tradicionalmente la vigilancia fundada en lo visual haya tenido una mayor importancia. La Comisión de Venecia incluyó un apartado específico a este tipo de vigilancia en la lista de control del EdD[168] con base en un dictamen específico sobre la videovigilancia en espacios públicos por las autoridades[169].

Según este dictamen de la Comisión de Venecia, la videovigilancia se define como «un sistema tecnológico de vigilancia por cámaras que puede ser elegido, instalado y utilizado por las autoridades en lugares públicos para la prevención de delitos o incluso la persecución del delito. El sistema suele consistir en un número de cámaras de vídeo que están conectadas en un circuito cerrado de televisión (CCTV). Las imágenes se envían a una televisión central y/o se graban. Comúnmente la instalación de CCTV incluye un número de cámaras conectadas a una sala de control en la que los operadores ven un banco de pantallas de televisión. Por lo tanto, el sistema de CCTV

165 *Ibid.,* apartado 84 y STJUE (Gran Sala) de 20 de septiembre de 2022 en los asuntos acumulados C-793/19 y C-794/19 SpaceNet AG y Telekom Deutschland GmbH; ECLI:EU:C:2022:702; apartado 113.

166 *Ibid.,* apartado 191.

167 *Ibid.,* partado 192.

168 Consejo de Europa, Comisión de Venecia, «Rule of law checklist» aprobada por el pleno de 11-12 de marzo de 2016; CDL-AD(2016)007rev, apartado F (2) d.

169 Comisión de Venecia del Consejo de Europa, dictamen CDL-AD(2007)014 sobre la videovigilancia en espacios públicos por autoridades públicas y la protección de los derechos humanos.

requiere la intervención de un ser humano para vigilar los monitores o revisar la grabación»[170]. Ha de tenerse en cuenta que el dictamen sobre videovigilancia fue elaborado en 2007 y desde entonces la tecnología ha evolucionado por la acumulación de varios avances disruptivos: el desarrollo de dispositivos cada vez más potentes, móviles, discretos y conectados en virtud de los avances en técnicas de miniaturización de sus elementos ópticos y electromagnéticos se ha sumado a los grandes avances que la inteligencia artificial ha aportado con el reconocimiento automatizado de imágenes, superando las capacidades distópicas de las telepantallas orwellianas[171].

El dictamen sobre videovigilancia define el espacio público como «aquel lugar al que, en principio, puede acceder cualquier persona de forma libre e indiscriminada, en cualquier momento y bajo cualquier circunstancia. *A priori*, cualquier persona puede usar de este tipo de espacios en cualquier momento. Los espacios públicos están regidos por las autoridades, cuyas facultades para hacer cumplir la ley e intervenir son más amplias que las de la propiedad privada. Algunos ejemplos de espacios públicos son los parques públicos, las calles peatonales en los centros de las ciudades, las zonas de aparcamiento público al aire libre, las calles de los barrios residenciales, zonas como estadios deportivos y estaciones de metro. Algunas zonas públicas como universidades, discotecas o cafeterías, que pueden considerarse zonas semipúblicas, también deben incluirse[172]». Sin embargo, el emplazamiento de una cámara de vigilancia en un espacio público no es neutro: la grabación de una masa de población en un estadio deportivo a los efectos de garantizar la seguridad del evento tiene distintas consecuencias que la grabación de una masa de ciudadanos en una avenida ejerciendo de modo legítimo su derecho de reunión y manifestación, ya que en este último caso el uso de esta tecnología por las autoridades, además de una injerencia en el derecho a la privacidad y a la protección de datos personales, puede resultar un factor desincentivador del ejercicio de otros derechos fundamentales[173].

---

170 Comisión de Venecia del Consejo de Europa, dictamen CDL-AD(2007)014 sobre la videovigilancia en espacios públicos por autoridades públicas y la protección de los derechos humanos. Apartado 13.

171 *Ibid.,* apartados 17 y 18; y Orwell, G. 1984; ed. Bilingüe del proyecto Gutenberg de Australia: «La telepantalla recibía y transmitía simultáneamente. Cualquier sonido que hiciera Winston superior a un susurro, era captado por el aparato. Además, mientras permaneciera dentro del radio de visión de la placa de metal, podía ser visto a la vez que oído. Por supuesto, no había manera de saber si le contemplaban a uno en un momento dado. Lo único posible era figurarse la frecuencia y el plan que empleaba la Policía del Pensamiento para controlar un hilo privado. Incluso se concebía que los vigilaran a todos a la vez. Pero, desde luego, podían intervenir su línea de usted cada vez que se les antojara. Tenía usted que vivir —y en esto el hábito se convertía en un instinto— con la seguridad de que cualquier sonido emitido por usted sería registrado y escuchado por alguien y que, excepto en la oscuridad, todos sus movimientos serían observados».

172 *Ibid.,* apartados 8 y 9.

173 Agencia de Derechos Fundamentales de la UE (FRA) hace una descripción detallada en su informe temático sobre la tecnología de reconocimiento facial (2019), capítulo 7.4.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

La lista de control del EdD propone, en coherencia con las conclusiones del estudio de videovigilancia, tres garantías básicas para el control de la videovigilancia por las autoridades[174]:

1.ª Que se realice con fundamento en necesidades de seguridad o para la prevención y control de delitos, y que se someta de hecho y de derecho a los requisitos fijados en el artículo 8 CEDH.

2.ª Que se informe a los ciudadanos de esta vigilancia en lugares accesibles al público.

3.ª Que se regule el acceso de los ciudadanos a cualquier videovigilancia que les afecte.

Las citadas garantías, de carácter genérico, vienen dadas tanto por la aplicación de la normativa de la UE en materia de protección de datos (en el caso del uso de la videovigilancia para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales sería de aplicación la Directiva (UE) 2016/680) como por la aplicación del convenio del convenio europeo STCE n.º 108+, que incluiría los tratamientos de videovigilancia con fines relacionados con la seguridad nacional.

La introducción de técnicas de procesamiento automatizado de datos biométricos y de patrones de comportamiento ha proporcionado un salto cualitativo sin precedentes en el nivel de intrusividad de la videovigilancia que requiere de la adopción de garantías adicionales. La técnica de reconocimiento biométrico más común en el ámbito de la videovigilancia es el reconocimiento facial, que se basa en el procesamiento automatizado de imágenes que contengan la cara de una persona con el fin de su verificación, de la identificación o de la categorización de un individuo mediante el uso de un patrón facial. Esta técnica pueda ser usada de modo retrospectivo, es decir, sobre una imagen de la cara tomada en un momento anterior al análisis automatizado o «en vivo», esto es, mediante el análisis de la imagen de cara tomada en tiempo real[175]. No obstante, también existen técnicas de procesamiento automatizado de otros datos biométricos, como las huellas dactilares y de la palma de la mano, el iris, la voz, e incluso características conductuales, como la manera de andar, o la expresión de emociones[176].

Aún más preocupantes resultan otros posibles usos de la biometría, como los derivados de determinadas aplicaciones de la neurociencia que demuestran la posibilidad de obtener información de los datos neuronales. Esta aplicación plantea nuevos retos que

174 Consejo de Europa, Comisión de Venecia, «Rule of law checklist» aprobada por el pleno de 11-12 de marzo de 2016; CDL-AD(2016)007rev, apartado F (2) (d).

175 La Agencia de Derechos Fundamentales de la UE (FRA) hace una descripción detallada en su informe temático sobre la tecnología de reconocimiento facial (2019), capítulo 3.

176 RGPD, artículo 4 (14) y «Biometric Recognition and Behavioural Detection» (2021). Estudio para el Parlamento Europeo; PE 696.968.

van más allá de la privacidad y que conectan la vigilancia con la libertad de pensamiento y opinión[177]. La amenaza distópica de una «policía del pensamiento»[178] ya ha sido abordada en Chile mediante una reforma constitucional que protege los datos neuronales[179] y también ha sido incluida en la Carta española de Derechos Digitales, que expresa que las condiciones, los límites y las garantías de implantación y empleo en las personas de las neurotecnologías podrán ser regulados por la ley con la finalidad de asegurar la confidencialidad y seguridad de los datos obtenidos o relativos a sus procesos cerebrales y el pleno dominio y disposición sobre los mismos[180].

El Comité del Convenio europeo STCE n.º 108+ ha adoptado unas directrices sobre este tipo de videovigilancia dirigidas al legislador y autoridades; a los desarrolladores, fabricantes y proveedores y a los usuarios de tecnologías de reconocimiento facial[181]. Entre las cautelas más destacadas, el Comité recomienda que, debido a su alto nivel de intrusividad, se restrinja estrictamente o incluso se prohíba completamente el uso del reconocimiento facial en tiempo real[182]. A esta misma conclusión llegaron las autoridades nacionales de protección de datos y el SEPD en su dictamen conjunto sobre la propuesta de reglamento de Inteligencia Artificial[183].

El Comité Europeo de Protección de Datos (CEPD), en sus directrices sobre el uso de la tecnología de reconocimiento facial en el ámbito policial, denuncia que la identificación biométrica a distancia de personas en espacios de acceso público supone un alto riesgo de riesgo de intrusión en la vida privada de los individuos y no tiene cabida en una sociedad democrática, ya que por su naturaleza implica una vigilancia masiva. En la misma línea, el CEPD considera que los sistemas de reconocimiento facial basados en el reconocimiento facial con ayuda de la IA, que clasifican a las personas en función de su biometría en grupos de acuerdo con la etnia y el género, así como la orientación política o sexual, no son compatibles con la CDFUE. Además, considera que el uso del reconocimiento facial o de tecnologías similares, para inferir las emociones de una

177 Consejo de Europa (2021). Informe de la comisión de Bioética (DH-BIO) «Common human rights challenges raised by different applications of neurotechnologies in the biomedical fields».

178 Orwell, G. 1984.

179 Ley chilena n.º 21.383, de 14 de octubre de 2021, por la que se modifica la carta fundamental para establecer el desarrollo científico y tecnológico al servicio de las personas.

180 Gobierno de España, Carta de Derechos Digitales (2021), XXVI.1.c).

181 Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108): Guidelines on facial recognition (2021).

182 *Ibid.,* p. 8.

183 Dictamen conjunto 5/2021 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de Inteligencia Artificial) de 18 de junio de 2021, apartado 31.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

persona física es altamente indeseable y debería prohibirse, posiblemente con algunas excepciones debidamente justificadas[184].

Aunque la noción de EdD se predica sobre la actividad tanto de autoridades como de sujetos privados, los puntos dedicados a la videovigilancia en la lista de control del EdD se formulan desde una perspectiva de la videovigilancia por autoridades. Sin embargo, la realidad demuestra que resulta relevante para el EdD la interacción de lo público y lo privado. Recientemente, se ha cuestionado el uso por autoridades públicas de numerosos Estados de las bases de datos de la empresa estadounidense Clearview AI, cuyo modelo de negocio consiste en vender a servicios de seguridad patrones biométricos útiles para el reconocimiento facial mediante un rastreo de millones de imágenes disponibles en redes sociales y en «otras fuentes digitales abiertas»[185]. Varias autoridades de protección de datos han considerado este tratamiento de datos biométricos contrario al Derecho de la Unión por haber introducido un cambio no consentido en la finalidad para que los usuarios de redes sociales cedieron su imagen a dichas redes[186], y que el hecho de que Clearview AI alegue (sin que exista prueba) que obtiene las imágenes faciales de fuentes abiertas, no quiere decir que el uso del producto obtenido por las aplicaciones de esta empresa pueda considerarse como fuentes de inteligencia abierta (en inglés *open source intelligence* —OSINT—). Las directrices del CEPD sobre el uso de la tecnología de reconocimiento facial en el ámbito policial también proscriben el tratamiento de datos personales en un contexto de policial mediante una base de datos elaborada con recopilación de datos personales a escala masiva y de forma indiscriminada, por ejemplo, mediante el «*scraping*»de fotografías e imágenes faciales accesibles en línea, en particular las que se ponen a disposición a través de las redes sociales, ya que este procedimiento no cumpliría, como tal, el requisito de necesidad estricta previsto en el Derecho de la Unión[187].

184 CEPD, Directrices 5/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito policial, apartado 118.

185 https://www.clearview.ai/overview.

186 SEPD (2021). EDPS Opinion on the possibility to use Clearview AI and similar services at Europol; Autoridad de control de Italia (Garante per la protezione dei dati personali) (2022) Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022 [9751362]; Autoridad de control de Suecia (Integritetsskyddsmyndigheten) (2021) Beslut efter tillsyn enligt brottsdatalagen – Polismyndighetensanvändning av Clearview AI.

187 CEPD, Directrices 5/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito policial, apartado 118 (*in fine*).

CONCLUSIÓN

La vigilancia es una actividad necesaria y al propio tiempo un riesgo grave para el Estado de derecho (EdD), ya que este se construye sobre los cimientos de la existencia de garantías legales e institucionales que prevengan el abuso de poder, y particularmente el abuso de la información como una forma de poder.

El vertiginoso avance de las tecnologías aplicadas a la vigilancia ha permitido que el nivel de intrusión sea mucho mayor, y la escala de la vigilancia alcance a un sector muy importante de la ciudadanía, siendo necesaria la existencia de un robusto sistema legal que transmita a esta la confianza sobre la efectividad de mecanismos de supervisión independientes que eviten el abuso de la información tanto por parte de las autoridades como por los particulares. En especial, la concentración del mercado de comunicaciones electrónicas en unos pocos proveedores de servicios ha incrementado el riesgo del abuso de estos datos por parte de actores no estatales introduciendo tratamientos para un fin distinto para el cual habían sido recopilados inicialmente, y que pueden tener graves consecuencias para el EdD, como han demostrado los escándalos de las empresas Cambridge Analytica y Clearview AI.

La existencia del doble marco regulatorio en materia de protección de datos personales en el ámbito de la UE y en el del Consejo de Europa permite someter al imperio de la ley a toda actividad de vigilancia realizada por operadores privados y por autoridades, incluida la realizada con finalidad de proteger la seguridad nacional, si bien la aplicación del derecho encuentra serias dificultades cuando la actividad de vigilancia se realiza sobre el flujo internacional de datos o cuando depende de entornos opacos y escasamente regulados, como el de las comunidades internacionales de servicios de inteligencia.

Los avances tecnológicos y el carácter ubicuo de dispositivos en red dotados de numerosos sensores hacen necesario limitar, de acuerdo con el principio de proporcionalidad, modalidades de vigilancia específica que resultan extraordinariamente intrusivas, como las que derivan del uso de programas espías similares al *spyware* Pegasus.

La vigilancia estratégica de las redes de telecomunicaciones está permitida con el fin de prevenir un riesgo real y grave de seguridad nacional, aunque sujeta a las salvaguardas de extremo a extremo que ha configurado la jurisprudencia del TEDH y del TJUE. Sin embargo, el uso de este tipo de vigilancia en el ámbito de la prevención y lucha contra la delincuencia grave debe estar sometido a mayor restricción bajo parámetros objetivos (categorías de datos), subjetivos (individuos o grupos de sospechosos), geográficos (espacios en los que el riesgo resulta superior), o de otro tipo que no causen discriminación.

La introducción de tecnologías disruptivas en la videovigilancia, como el reconocimiento automatizado de datos biométricos (en particular el reconocimiento facial) y su uso por las autoridades en lugares públicos, debe estar sujeta a las mayores cautelas, con prohibición del empleo de esta tecnología en tiempo real con el fin de proteger la libre

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

circulación de ciudadanos inocentes en el ejercicio de otros derechos fundamentales esenciales para el EdD, como la libertad de reunión y manifestación. Las amenazas al EdD pueden ser aún mayores con la aplicación de la neurotecnología a la vigilancia, que puede comprometer no solo la esencia de la intimidad y la protección de datos, sino también la libertad de pensamiento, por lo que debería realizarse una mayor apuesta en la comunidad internacional y académica en la protección de los neuroderechos[188] frente a la vigilancia.

188 *Vid.,* la iniciativa del científico español Rafael Yuste a través de la Neurorights Foundation.

BIBLIOGRAFÍA

Azoulai, Loïc; Ritleng, Dominique: «L'État, c'est moi». Le Conseil d'État, la sécurité et la conservation des données, Revue trimestrielle de droit européen 2021, p.p 349-379.

Baartmans, Chloë; Cox, Manuela: De nasleep van Schrems II houdt niet over: de gevolgen van de uitspraak van het HvJ EU in Schrems II en de daaropvolgende (concept) aanbevelingen van de EDPD onder de loep genomen, Mediaforum: Tijdschrift voor Media- en Communicatierecht 2021 n.º 1 pp. 2-7.

Bahamonde Blanco, Miriam; Primeras impresiones sobre la Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2020, en los asuntos La Quadrature du Net y otros, y sus efectos en la Investigación Penal en España; Diario La Ley, ISSN 1989-6913, n.º 9733, 2020.

Bergholm, Jenny: The Data Retention Saga Continued – from Tele2 Sverige to Privacy International and La Quadrature du Net, Tidskrift Utgiven av Juridiska föreningen i Finland 2021 Vol. 2 pp. 111-139.

Brunessen, Bertrand: Les enjeux de la surveillance numérique, Revue trimestrielle de droit européen 2021, n.º 1, pp. 175-180.

— Le champ d'application du droit européen du numérique, Revue trimestrielle de droit européen 2021, n.º 1, pp. 181-187.

Caiola, Antonio: Transmission et conservation des données en rapport avec la sécurité nationale: précisions et nuances émergeant dans la jurisprudence / Transmission and retention of data in relation to national security: clarifications and nuances emerging in case law, Revue des affaires européennes 2020 n.º 4 pp. 923-933.

Cameron, Iain: Metadata retention and national security: Privacy International and La Quadrature du Net: Case C-623/17, Common Market Law Review 2021 pp. 1433-1472.

Castets-Renard, Céline: Cour de justice, 16 juillet 2020, Data Protection Commissioner c/ Facebook Ireland Ltd, Maximillian Schrems, aff. C-311/18, ECLI:EU:C:2020:559, Jurisprudence de la CJUE 2020. Décisions et commentaires 2020, pp. 1080-1090.

— Cour de justice, gde ch., 6 octobre 2020, La Quadrature du Net e. a., aff. jtes C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:791, Jurisprudence de la CJUE 2020. Décisions et commentaires 2020, pp. 1091-1100.

Cellerino, Chiara: Trasferimenti internazionali di dati personali e clausole contrattuali tipo dopo Schrems II: C-311/18, Data Protection Commissioner c. Facebook Ireland e Schrems (Schrems II), Il diritto dell'Unione Europea 2021 pp. 351-320.

D'Ath, Florence: Arrêt «Schrems II»: sur la légalité des transferts de données personnelles fondés sur une décision d'adéquation ou moyennant des garanties appropriées, Journal de droit européen 2020 n.º 10 pp. 442-445.

De Terwangne, Cécile: L'illégalité nuancée de la surveillance numérique: la réponse des juridictions belge et française à l'arrêt La Quadrature du Net de la Cour de justice de l'Union européenne, Revue trimestrielle des droits de l'homme 2022 n.º 129 pp. 3-27.

Deroudille, Alexis: L'arrêt Schrems II, vers une résolution de l'équation transatlantique?, Revue de l'Union Européenne 2021 n.º 3 pp. 144-162.

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

Dworschak, Marco: Auswirkungen von Schrems II auf den Steuerdatentransfer, Liechtensteinische Juristen-Zeitung 2020 Abh. pp. 295-309.

Eskens, Sarah Johanna: The ever-growing complexity of the data retention discussion in the EU: an in-depth review of La Quadrature du Net and others and Privacy International: joined cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net and others [2020], case C-623/17 Privacy International, European Data Protection Law Review 2022 Vol. 8 n.º 1 pp. 143-155.

Flett, Emma; Jenny; Clover, Jacqueline: Schrems strikes again: EU-US privacy shield suffers same fate as its predecessor, Computer and Telecommunications Law Review 2020 pp. 161-163.

FRA (2015) Surveillance by intelligence services - Volume I: Member States' legal frameworks.

FRA (2017) Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update.

FRA (2018) Manual de legislación europea en materia de protección de datos.

FRA (2019) Facial recognition technology: fundamental rights considerations in the context of law enforcement.

Jacques, Florian: «Uncle Sam is watching you» Retour sur les enseignements de l'arrêt Schrems II de la Cour de justice de l'Union européenne, Journal des tribunaux 2021 pp. 246-249.

Kuner, Christopher; Bygrave, Lee; Docksey, Christopher; Drechsler, Laura: The EU General Data Protection Regulation (GDPR): A Commentary; Oxford (2020).

Meltzer, Joshua P.: After Schrems II: The Need for a US-EU Agreement Balancing Privacy and National Security Goals, Global Privacy Law Review 2021, pp. 83-89.

Nebbia, Paolisa: The Schrems judgments: a silent revolution for Member States' procedural autonomy?: C-362/14 and C-311/18, ERA-Forum: scripta iuris europaei 2021 pp. 327-336.

Nino, Michele: La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE, Il diritto dell'Unione Europea 2021 pp. 93-124.

Lobato Cervantes, Virgílio Emanuel: The Schrems II judgment of the Court of Justice invalidates the EU-U.S. privacy shield and requires «case by case» assessment on the application of Standard Contractual Clauses (SCCs): Case C-311/18 Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, European Data Protection Law Review 2020 Vol. 6 n.º 4 pp. 602-606.

Pau, Antonio y Hernando Grande, Antonio: «La cibercosmología como premisa del ciberderecho», Boletín del Ministerio de Justicia, Año LXXV, Núm. 2.236, enero de 2021.

Rojszczak, Marcin: National security and retention of telecommunications data in light of recent case law of the European Courts, European Constitutional Law Review 2021 Vol. 17 Issue 4 pp. 607-635.

Rotenberg, Marc: Schrems II, from Snowden to China: toward a new alignment on transatlantic data protection, European Law Journal: review of European law in context 2020 pp.141-152.

Ruiz Dorado, María; Constitución y Espionaje (2022), Ed. Tirant lo Blanch.

Sandfuchs, Barbara: The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II, Gewerblicher Rechtsschutz und Urheberrecht INT 2021 pp. 245-249.

Sellars, Clare: Schrems II and Standard Contractual Clauses – the Advocate-General's Opinion, Computer Law Review International 2020 pp. 29-30 .

Simon, Denys: Droits fondamentaux - Protection des données, Europe 2020, n.º 12 Décembre, Comm. 374.

— Coup de tonnerre dans le monde du numérique. La Cour de justice prononce l'invalid Wilson ité du «bouclier de protection de la vie privée» à propos des transferts de données personnelles vers les États-Unis, Europe 2020, n.º 8-9 Août, étude 8, pp. 5-10.

Sirinelli, Jean: La protection des données de connexion par la Cour de justice: cartographie d'une jurisprudence européenne inédite, Revue trimestrielle de droit européen 2021, n.º 2, pp. 313-330.

Snoy, Ophélie: Transfert de données à caractère personnel de l'Europe vers un pays tiers: état des lieux à la suite de la décision «Schrems 2 », Revue de droit commercial belge 2021 n.º 5 pp. 581-596.

Sobrino García, Itziar: Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y Estados Unidos, Revista de Derecho Comunitario Europeo 2021 n.º 68 pp. 227-256.

Tambou, Olivia: L'invalidation du Privacy Shield: peut-on sortir des turbulences dans les flux transatlantiques des données à caractère personnel?, Revue trimestrielle des droits de l'homme 2021 n.º 125 pp. 153-166.

Thiele, Clemens: Ist der Datentransfer in die USA am Ende? - Zur Unzulässigerklärung des EU Privacy Shield - Analyse der Entscheidung EuGH 16. 7. 2020, C-311/18 mit Praxistipps, JusIT: IT-Recht, Rechtsinformation, Datenschutz 2020 pp. 196-198.

Tinière, Romain: Cour de justice, gde ch., 6 octobre 2020, La Quadrature du Net e.a., aff. jtes C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:791, Jurisprudence de la CJUE 2020. Décisions et commentaires 2020, pp. 130-139.

Tracol, Xavier: Chapter V of Regulation (EU) 2018/1725 on transfers of personal data by Union institutions and bodies to third states and international organisations, ERA-Forum: scripta iuris europaei 2021 pp. 00.

— Schrems II: the return of the privacy shield, Computer law & security review 2020, pp. 1-11.

Tzanou, Maria; Karyda, Spyridoula: Privacy International and Quadrature du Net: one step forward two steps back in the data retention saga?: case C-623/17 Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others , joined cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net

Fecha de recepción: 22-07-2022. Fecha de aceptación: 30-09-2022

and Others v. Premier Ministre and Others, European Public Law 2022 pp. 123-154.

Vander, Sascha: Datenschutzkonforme Datenexporte in Drittländer: Empfehlungen der Aufsichtsbehörden und Entwurf neuer Standardvertragsklauseln: C-311/18, Der Betrieb 2021 pp. 214-218 .

Zalnieriute, Monika: A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union, The Modern Law Review 2022, n° 1, pp. 198-218.

Maquetación:
Ministerio de Justicia
Secretaría General Técnica
Subdirección General de Documentación y Publicaciones