Anuario de la Facultad de Derecho. Universidad de Extremadura 39 (2023): 51-68
ISSN: 0213-988X – ISSN-e: 2695-7728

Doi: https://doi.org/10.17398/2695-7728.39.51

CONSERVACIÓN Y ADQUISICIÓN DE DATOS EXTERNOS DE COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS: BUSCANDO UN EQUILIBRIO ENTRE SEGURIDAD Y LIBERTAD

RETENTION AND ACQUISITION OF EXTERNAL DATA FROM TELEPHONE AND TELEMATIC COMMUNICATIONS: STRIKING A BALANCE BETWEEN SECURITY AND FREEDOM

ELENA AUGUSTA ANDOLINA[1]

Università degli Studi "Magna Graecia" de Catanzaro. Italia

Recibido: 01/11/2023 Aceptado: 05/12/2023

RESUMEN

El artículo analiza la compleja evolución de la legislación italiana en materia deretención y adquisición de datos identificativos de las comunicaciones telefónicas/ telemáticas para la represión de delitos. Tradicionalmente considerada como una metodología de investigación con una modesta capacidad intrusiva, ha demostrado ser cualquier cosa menos neutral con la revolución tecnológica. Aunque ajeno a los contenidos comunicativos, en realidad es adecuado para atacar un amplio marco de derechos fundamentales (el derecho al secreto, a la intimidad y a la protección de datos personales). Solo después de la enésima sentencia del Tribunal de Justicia de la Uníon

[1] Profesora de Derecho Procesal Penal en la Universidad "Magna Graecia" de Catanzaro (Italia). Ha realizadoestancias de investigación en Universidades espagnolas (Universidad de Vigo y Universidad de Extremadura). Las principales líneas de investigación son: cooperación sudicia penal, victima vulnerabile, violencia de genero, justicia restaurativa, interceptaciones de conversaciones o comunicaciones, investigaciones encubiertas, derecho al silencio del acusado.

Europea, el legislador italiano reformó el regime regulatorio, pero solo limitado a la adquisición de datos de comunicaciones externas. Sin embargo, todavía esiste otros aspectos de fricción con el derecho de la UE con respecto al aspecto específico de la conservación de datos y el de la adquisición de datos externos con fines preventivos.

Palabras clave: Derechos Humanos (el secreto de las comunicaciones – derecho a la intimidad y protección de datos personales-Conservación y Adquisición de datos del tráfico telefónico), Proceso penal,Tribunal europeo de Derechos Humanos, Tribunal de Justicia de la Uníon Europea.

ABSTRACT

The article analyzes the complex evolution of Italian legislation regarding the archiving and acquisition of identification data of telephone/telematiccommunications for the suppression of crimes. Traditionally regardedas a survey methodology with modest intrusive capacity, it has proven to be anything but neutral with the technological revolution. Although unrelated to comunicative content, it is actually suitable for attacking a broad framework of fundamental rights(the right to secrecy, privacy and protection of personal data). Only after the umpteenth ruling of the Court of Justice of the EU did the Italian legislator reform the regulatory regime, butonly limited to the acquisition of data from external communications. However, there are still other aspects of friction with EU law regarding the specific aspect of data retention and the acquisition of external data for preventive purposes.

Keywords: Human Rights (the secrecy of communications - right to privacy and protection of personal data),Conservation and Acquisition of telephone traffic data, Criminal procedings, Tribunal Europeo de Derechos Humanos, Tribunal de Justicia de la Unión Europea.

Sumario: 1. Límites a la retención y adquisición de datos de tráfico telefónico y telemático en el Derecho Vivo de la Unión Europea. 2. El art. 132 Código de Privacidad en la versión anterior a la ley de reforma 178/2021, de 23 de noviembre. 3. El aumento exorbitante de los tiempos de retención de los datos de tráfico. 4. La sentencia H. K. c. Prokuratuur: un punto de no retorno en la polémica sobre la conservación de datos. 5. El nuevo régimen de accesibilidad a los datos "externos" de las comunicaciones telefónicas y electrónicas. 6. La reforma del art. 132 Código de Privacidad: sólo una adaptación parcial a la legislación de la UE. Referencias bibliográficas.

1. LÍMITES A LA RETENCIÓN Y ADQUISICIÓN DE DATOS DE TRÁFICO TELEFÒNICO TRÁFICO Y TELEMÁTICO EN EL DERECHO VIVO DE LA UNIÓN EUROPEA

La adquisición posterior de datos "externos" que identifican las comunicaciones telefónicas (números de usuario emisor y receptor, fecha, hora, duración y lugar de la comunicación en el caso de teléfonos móviles) puede dar lugar a violaciones importantes de los derechos fundamentales de la persona, por parte del organismo gestor del servicio telefónico en el denominado registros telefónicos (o electrónicos). Aunque no estén relacionados con los contenidos de la comunicación, estos datos agregados con herramientas informáticas proporcionan, de hecho, indicaciones muy precisas sobre la vida privada de la persona (como hábitos, movimientos, relaciones personales y profesionales).

Tradicionalmente considerada como una metodología de investigación con poca capacidad intrusiva o incluso neutral, esta técnica de control telefónico ha visto aumentar su invasividad en correspondencia con la revolución tecnológica de la era digital y la expansión de la telefonía móvil; con la consiguiente ampliación del marco de derechos fundamentales sacrificados.

Tanto la jurisprudencia del Tribunal Constitucional italiano como el de los Tribunales europeos (Tribunal Europeo de Derechos Humanos y Tribunal de Justicia de la Unión Europea) han contribuido a la progresiva identificación de los valores implicados en esta herramienta de investigación. Por un lado, el derecho al secreto sobre el hecho histórico de la comunicación, es decir, a mantener en secreto los datos identificativos de la relación de comunicación distintos del contenido de la conversación telefónica en sí, ha sido devuelto desde hace mucho tiempo por el Tribunal Constitucional italiano al ámbito de la garantía del articulo 15 de la Constitución[2]; por otro, el derecho a la protección de la esfera privada y el derecho a la libre determinación de los datos personales protegidos en las fuentes europeas de derechos humanos - art. 8 del Convenio Europeo de Derechos Humanos y los artículos 7- 8 de la Carta de Derechos Fundamentales de la Unión Europea, tal como la interpretaron los jueces de Estrasburgo y Luxemburgo.

[2] Tribunal Constitucional italiano. Sentencia nùm. 81/1993, de 11 de marzo, en *Giurisprudenza costituzionale* (1993): 736, con comentario de Pace Alessandro.

En concreto, sin embargo, fue la jurisprudencia del Tribunal de Justicia de la Unión Europea la que definió progresivamente los límites al almacenamiento y adquisición de datos de tráfico.

El punto de partida es la famosa sentencia Digital Rights Ireland y Seitlinger (de 8 de abril de 2014)[3] con la que los jueces de Luxemburgo anularon la Directiva UE 2006/24 (la llamada directiva Frattini), relativa a la conservación generalizada e incondicional de los datos de tráfico, por parte de los proveedores, con fines de prevención y represión de delitos graves - por el grave sacrificio de la esfera privada que excede el principio de proporcionalidad en términos de estricta necesidad.

Después de haber destacado el carácter "cualificado" - o "más que personal"[4] - de los metadatos generados por las comunicaciones electrónicas, que permiten reconstruir esferas enteras de relaciones personales y sociales a lo largo del tiempo de personas cuyos datos han sido almacenados, el Tribunal resolvió que esta grave intromisión, para ser razonable, debe ser contrarrestada por una regulación que, por el lado de la adquisición, limite el acceso a los datos en función del objetivo de luchar contra los delitos graves; sometiéndolo también a condiciones sustantivas y procesales precisas, así como a un control previo por parte del juez o de una autoridad administrativa independiente.

Los principios de garantía de la sentencia sobre derechos digitales fueron reiterados, también en lo que respecta a las normativas nacionales, en la sentencia *Tele 2 Sverige y Watson* 5, en la base de una lectura constitucionalmente orientada de la Directiva (UE) 2002/58 (relativa a la privacidad electrónica) que se convirtió en la única fuente regulatoria actual de la Unión Europea sobre retención de datos. Habiendo excluido la compatibilidad de las leyes nacionales que establecen un régimen general e indiferenciado para la conservación de todos los datos relativos a las comunicaciones electrónicas, se precisó que el art. 15, párr. 1, de la citada Directiva (UE) no es un obstáculo para la retención y el acceso "dirigidos" a datos de tráfico y de localización, con el fin de luchar contra delitos graves", cuando dicho procesamiento esté "limitadoen la medida estrictamente necesaria", con respecto a las categorías de datos, medios de comunicación y interesados, así como a la duración de la comunicación.

---

[3] Tribunal de Justicia de la Unión Europea. Sentencia de 8 abril 2014, *Digital Rights Ireland e a. c. Minister for Communications,* asuntos C-293/12 e C-594/12, en http://archiviodpc.dirittopenaleuomo .org, con comentario de Flor Roberto.
[4] Conclusiones del Abogado General UE *Pedro Cruz Villalon,* asuntos C-293/12 e C-594/12.

2. EL ARTICULO 132 CÓDIGO DE PRIVACIDAD EN LA VERSIÓN ANTERIOR A LA LEY DE REFORMA 178/2021, DE 23 DE NOVIEMBRE

Los principios de las sentencias Digital Rights y Tele2Sverige pusieron en duda la legitimidad y, por tanto, la "sostenibilidad" de las estructuras regulatorias internas para el archivo y la adquisición indiscriminada de datos de tráfico. De esta manera, resulta inválido e inaplicable por los jueces nacionales, por entrar en conflicto con el derecho primario europeo el régimen previsto en el articulo 132 del Decreto Legislativo 196/2003, de 30 de junio ("Código de protección de datos personales", el llamado Código de Privacidad), modificado por el Decreto Legislativo 109/2008, de 30 mayo, que implementa la directiva 2006/24.

De hecho, la legislación italiana que transpone la directiva Frattini presentaba claros puntos de fricción con el canon de proporcionalidad.

El citado artículo 132 imponía la conservación "a efectos de comprobación y represión de delitos" de los datos relativos al tráfico telefónico "durante veinticuatro meses a partir de la fecha de su comunicación"; así como, "con las mismas finalidades", el de los datos relativos al tráfico electrónico "durante doce meses desde la fecha de la comunicación" y el de los datos relativos a llamadas no atendidas "durante treinta días" (párrafos 1 y 1-bis del artículo 132 Código de Privacidad).

Este régimen de conservación sistemático e indiscriminado, previsto en relación con todos los datos de tráfico y localización, con todos los medios de comunicación electrónica, así como con todos los abonados y/o usuarios registrados, sin límites ni excepciones de ningún tipo, no fue, sin embargo, reequilibrado por una regulación suficientemente precisa en materia de adquisición de datos; dada la falta de certeza no sólo de las condiciones específicas que legitiman la restricción del secreto, sino también de los tipos de delitos graves en los que se basa el acceso a los propios datos. De hecho, se permitía, como consecuencia del aplazamiento realizado por el apartado 3 del art. 132 en el párrafo 1 anterior, la accesibilidad a los datos de tráfico, mediante decreto motivado del Ministerio Público, independientemente de criterios objetivos precisos adecuados para limitar dicho acceso a lo estrictamente necesario - con la consiguiente emisión automática del decreto de adquisición - y, por otra parte, para fines genéricos de investigación y represión de los delitos (apartado 1 del art. 132). Precisamente la extrema indeterminación de esta referencia normativa, totalmente inadecuada para identificar los casos específicos de delitos "graves" respecto de los cuales delimitar dicho acceso, permitía obtener datos a los efectos de la in-

vestigación penal de cualquier hipótesis de delito, incluso leves; en conflicto, tanto con el principio de legalidad, como con la limitación de la referencia de la finalidad perseguida.

3. EL AUMENTO EXORBITANTE DE LOS TIEMPOS DE RETENCIÓN DE LOS DATOS DE TRÁFICO

Después de las sentencias, Digital Rights y Tele 2 Sverige, integrantes de un verdadero "Estatuto Europeo" de herramientas de vigilancia predestinadas a la recogida de datos "externos" al contenido de la comunicación, el legislador debería haber revisado toda la reglamentación de acuerdo con las garantías de legalidad, jurisdicción y proporción.

Por otrolado, no sólo no se ha producido una intervención rejuvenecedora inmediata para adaptarse a los estándares europeos, sino que se han adoptado medidas regulatorias con una acentuada inspiración de seguridad con la que, bajo la presión de la creciente amenaza del terrorismo global, se ha conseguido una importante, y muy preocupante, ampliación de los tiempos de almacenamiento en claro contraste con el canon de la proporcionalidad. Con el fin de garantizar la eficacia de los instrumentos de investigación en vista de las necesidades extraordinarias de la lucha contra el terrorismo internacional, el legislador italiano ha intervenido, con el art. 24 de la Ley Europea 167/2017, de 20 de noviembre, que desarrolla el art. 20 de la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo, que eleva el período de conservación de los datos telemáticos telefónicos (así como de los intentos de llamadas no contestadas) a setenta y dos meses (¡lo que equivale a seisaños!).

Este régimen, concebido originalmente en una perspectiva de emergencia y excepcionalidad, ha pasado a ser ordinario, habiéndose transfundido en el nuevo párrafo 5-bis del art. 132 del Código de Privacidad 196/2003, de 30 juno, modificado por el art. 11 del Decreto Legislativo 101/2018, de 10 de agosto.

La intención del legislador era introducir un régimen dual de conservación-adquisición, diferenciado en función del delito perseguido. Previendo, para los delitos comunes, un plazo de archivo articulado de veinticuatro meses, doce meses y treinta días -en función del origen de los datos- y, para los delitos graves de carácter terrorista, un plazo de conservación homogéneo de setenta y dos meses, con independencia del origen de los datos tratados.

Sin embargo, tal discrepancia en los períodos de conservación de los datos de tráfico no es factible en la práctica[5].

De hecho, el operador, al no poder conocer ex ante para qué tipo de delitos serán solicitados los datos por el Ministerio Fiscal, estará obligado a conservar la gran cantidad de datos generados por las comunicaciones –vía telefónica, Internet o llamadas no contestadas- durante un plazo de seis años.

Por lo tanto, si sobre la base de los apartados 1, 1 bis y 5 bis del art. 132 del Código de Privacidad 196/2003, el tiempo ordinario de conservación de los datos telefónico-telemáticos es ahora igual a seis años, por lo que es evidente que, desde este punto de vista, el marco normativo italiano no está exento de graves denuncias de incompatibilidad con el derecho unitario europeo. Se trata, en efecto, de un período unitario de supresión que evidentemente no es "adecuado"[6] y va en detrimento del derecho al olvido; así como excede el límite de estricta necesidad impuesto por el canon de proporcionalidad.

4. LA SENTENCIA H. K. C. PROKURATUUR: UN PUNTO DE NO RETORNO EN LA POLÉMICA SOBRE LA CONSERVACIÓN DE DATOS

El proceso de definición progresiva del delicado equilibrio entre las exigencias de seguridad y el derecho al respeto de la vida privada encuentra un desarrollo coherente en la sentencia del Tribunal de Justicia de la Unión Europea, relativa al caso H.K. c. Prokuratuur[7]; lo que marca un punto de inflexión fundamental en la dirección de garantizar el marco normativo interno. En esta sentencia, el Tribunal de Luxemburgo ha examinado, de conformidad con los principios de legalidad y proporcionalidad, aspectos que aún no han sido sufficientemente explorados.

En resumen, la sentencia controvertida tiene su origenen una cuestión de prejudicialidad planteada por el Riigikohus (Tribunal Supremo de l.o Civil y

[5] Como se señaló de inmediato en la doctrina: Signorato Silvia, "Novità in tema di Data retention. La riformulazione dell'art. 132 Codice Privacy da parte del d.lgs. 10 agosto 2018, n. 101",en http://archiviodpc.dirittopenaleuomo.org;
Baccari Gian Marco, "Il trattamento (anche elettronico) dei dati personali per finalità di accertmento dei reati",en *Cybercrime,* dir. por Cadoppi Alberto et al. (Torino: Utet, 2019): 1881.

[6] Esto es contrario al artículo 5 (Períodos de conservación y examen) de la Directiva 2016/680/UE, que establece la obligación de los Estados de establecer «plazos adecuados para la supresión de los datos personales».

[7] Tribunal de Justicia de la Unión Europea. Sentencia de 2 marzo 2021, asunto C-746/18, *H.K c. Prokuratuur*, en https://www.processopenaleegiustizia.it, con comentario de Andolina Elena.

Penal, Estonia), que planteó tres cuestiones prejudiciales al Tribunal de Justicia de la Unión Europea. Más concretamente, preguntó si - con arreglo al artículo 15, apartado 1, de la Directiva (UE) 2002/58, interpretado a la luz de los artículos 7, 8, 11 y 52 de la Carta de Derechos Fundamentales de la Unión Europea - el objetivo de luchar contra la delincuencia en general puede justificar el acceso a los datos de tráfico almacenados por los proveedores si la duración de dicho acceso es corta o la cantidad de datos recopilados es muy limitada; si las pruebas obtenidas, contrarias al Derecho de la Unión, son admisibles y apreciables en el marco de un procedimento penal;y, por último; si el Prokuratuur (Ministerio Fiscal) es una autoridad «independiente» en el sentido de la sentencia Tele2 Sverige y Watson.

Con respecto a las dos primeras cuestiones, las sentencias del Tribunal de Justicia de la Unión Europea recordaron los principios de derecho ya establecidos en la materia, desarrollando sus implicaciones lógicas.

Por lo que respecta a las razones que justifica nel acceso a los datos conservados por los proveedores de servicios de comunicaciones electrónicas, el Tribunal de Justicia de la Unión Europea, sobre la base del criterio tripartito que impliqua el principio de proporcionalidad, reiteró que la licitud de la restricción de la intimidad «debe apreciarse midiendo la gravedad de la injerencia que dicha limitación implica y comprobando que la importancia del objetivo de interés general perseguido por [el primero] está relacionada con la gravedad de la injerencia»[8].

Más concretamente, de acuerdo con el límite de necesidad previsto en el artículo 52 de la Carta de Derechos Fundamentales de la Unión Europea, el equilibrio entre el objetivo de interés general y los derechos fundamentales afectados por la medida exige que la injerencia sea estrictamente proporcionada al objetivo perseguido o, en otras palabras, que exista una correspondencia entre el grado de intensidad de la injerencia en las libertades individuales que sea perjudicial para el interés perseguido.

En consecuencia, cuantomás intenso es el sacrificio impuesto a la esfera subjetiva del individuo, mayor debe ser el "peso" del interés general quejustifica la injerencia en la esfera individual[9].

[8] STJUE, asunto C-746/18, párr. 31 y 32.
[9] Negri Daniele, "Compressione dei diritti di libertà e principio di proporzione davanti alle sfide del processo penale contemporaneo", en *Rivista italiana di diritto e procedura penale* (2020): 3.

Sobre esta base, el Tribunal de Luxemburgo, por un lado, reafirmó el principio de que solo la lucha contra la delincuencia grave (o la prevención de amenza graves para la seguridad pública) puede justificar injerencias graves en los derechos fundamentales previstos en los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea, como las derivadas de la conservación y recogida de datos de tráfico o de localización; independien-temente de otros factores relacionados con la duración del período durante el cual se solicita el acceso a dichos datos, la cantidad o la naturaleza de los datos disponibles durante dicho período. En segundo lugar, reiterò que solo las injerencias no graves, como las resultantes del tratamiento de datos relativos a la identica civil de los usuarios de medios de comunicación electrónicos, pueden justificarse por el objetivo de prevención, detección y persecución de las infracciones penales en general, establecido en el artículo 15, apartado 1, de la Directiva (UE) 2002/58. Dado que estos datos no permiten conocer la fecha, la hora, la duración y los destinatarios de las comunicaciones realizadas, ni el lugar o la frecuencia de dichas comunicaciones, no proporcionan ninguna información sobre las comunicaciones realizadas y, por tanto, sobre su vida privada»[10].

Por lo que se refiere a la cuestión de la inadmisibilidad como prueba de los informes de datos de tráfico y de localización obtenidos sobre la base de una normativa incompatible con el Derecho de la Unión Europea, tanto en lo que respecta a la conservación generalizada e indiferenciada de los datos como a los métodos de acceso a los mismos, la postura del Tribunal de Justicia de la Unión Europea se caracteriza por una cierta cautela.

Por una parte, se recordó que «en el estado actual del Derecho de la Unión, corresponde exclusivamente al Derecho nacional establecer las normas relativas a la admisibilidad y a la apreciación, en el marco de un proceso penal, de las pruebas «obtenidas en contra del Derecho de la Unión»; ya que, a falta de normas comunitarias específicas en la materia, corresponde a la competencia autónoma de los Estados miembros (en virtud del artículo 19 TUE) elegir las vías de recurso adecuadas para garantizar el respeto de los derechos de origen europeo en los ámbitos cubiertos por el Derecho de la Unión Europea.

Subrayando que dicha autonomía procesal debe ejercerse dentro de los límites marcados por el respeto de los principios de equivalencia de trato —entre las infracciones del Derecho de la Unión y las del Derechonacional— y de

[10] STJUE, asunto C-746/18, párr. 33 a 35.

efectividad del Derecho UE[11].

Es precisamente el principio de efectividad el que obliga al juez penal nacional a excluir las pruebas obtenidas, en el marco de un proceso penal, infringiendo el Derecho de la Unión Europea; cuando la admisibilidad y la utilidad de dichas pruebas puedan causar un perjuicio indebido a la persona acusada de una infracción penal, desde el punto de vista del respeto del principio de contradicción y, por tanto, del derecho a un proceso equitativo, impidiéndole hacer efectivas sus inferencias sobre los elementos de prueba antes mencionados[12].

Por lo que respecta a la tercera cuestión prejudicial, el Tribunal de de Luxemburgo, al ser solicitado sobre la legitimidad del Ministerio Fiscal para autorizar, con fines de investigación, el acceso a los datos de tráfico y localización, precisó los criterios que debe cumplir una autoridad nacional para ser considerada "independiente".

También en este aspecto, los principios del Tribunal[13] son el corolario lógico del cumplimiento del criterio de proporcionalidad, en el que debe basarse el equilibrio racional entre las necesidades de investigación perseguidas y la protección de los derechos individuales en juego. Sobre la base de este criterio, el reconocimiento de la capacidad de perjuicio acentuada del almacenamiento y la recogida de datos de tráfico implica queel acceso no solo debe estar respaldado por una justificación reforzada, sino también por condiciones sustanciales de procedibilidad idóneas para garanti zar que la ingerencia en sus derechos fundamentales no se haga sin ellímite de la estricta necesidad.

El pleno respeto de estos parámetros exige - como señala el Tribunal de Justicia de la Unión Europea - «que el acceso de las autoridades nacionales competentes a los datos conservados esté sujeto a un control previo efectuado

---

[11] Peraro Cinzia, "L'autonomia procedurale degli Stati membri alla prova della Carta dei diritti fondamentali", *Annali AISDUE* (2020), in https://www.aisdue.eu, en elque se señala que el principio de autonomía procesal está «sujeto a un equilibrio con otros principios fundamentales, como la equivalencia y la efectividad, que son los parámetros de referencia de las disposiciones procesales internas».
[12] STJUE, asunto C-746/18, párr. 44.
[13] Disipando así las dudas interpretativas generadas por el uso de los términos "jurisdicción" -en la versiónfrancesa- y "court" -en la versión inglesa-, entendidos, incluso recientemente, por Tribunal de Casación italiana en un sentido promiscuo, es decir, tal que incluye tanto al juez como al fiscal (seccion II de sentencia de 10 dicembre de 2019, n. 5741, in Casación ced, n. 278568; seccion III de sentencia de 19 de abril de 2019, n. 36380, in *Sistema penale,* n. 5 (2020): 5, con comentario de Neroni Rezende Isadora, https://www.sistemapenale.it; e in *Diritto di Internet,* n. 4 (2019): 753, con comentario de Luparia Luca, https://dirittodiinternet.it).

por un órgano jurisdiccional o por un órgano administrativo independiente»; que «presenta todas las garantías necesarias para garantizar la conciliación de los distintos intereses y derechos en juego». Se precisa que, cuando tal control es ejercido «por una entina administrativa independiente, dicha entina debe gozar de un estatuto que le permita actuar con objetividad e imparcialidad en el ejercicio de su misión, de modo que esté libre de toda influencia externa»[14].

Es, por tanto, la «exigencia de independencia» la que impone la imparcialidad -respecto de la que solicita el acceso a los datos- de la autoridad encargada de ejercer el control previo; y de scartar que "esté involucrado en la realización de la investigación penal"[15].

Precisamente los dos parámetros en los que se traduce la independencia - la impermeabilidad a los elementos externos que pueden influir en las decisiones; y la capacidad de satisfacer, en virtud de las funzione que le han sido encomendadas, una exigencia de objetividad en el marco del control queejerce– no existenen un fiscal que dirige las investigaciones penales y asume, en caso de enjuiciamiento, la condición de parte en el proceso.

En efecto, no basta con que, a efectos de la imparcialidad respecto de los intereses en juego, el Ministerio Fiscal esté obligado a actuar únicamente en el plano jurídico.

Así, se ha aclaradoque, de acuerdo con el art. 15 de la Directiva (UE) 2002/58, solo la intervención preventiva de un organismo «por encima de toda sospecha de parcialidad»[16], como los tribunales, puede garantizar un control riguroso de la medida que invade la esfera privada, capaz de limitar el acceso a los datos almacenados dentro del límite de racionalidad impuesto por el canon de proporcionalidad y, por tanto, de frenar el peligro de abuso y/o de injerencia arbitraria.

5. EL NUEVO RÉGIMEN DE ACCESIBILIDAD A LOS DATOS "EXTERNOS" DE LAS COMUNICACIONES TELEFÓNICAS Y ELECTRÓNICAS

Una vez rechazado el supuesto de la capacidad invasiva reducida del instrumento en cuestión - en la base del régimen no protector previsto en el art. 132 del Código de Privacidad 196/2003 - se confirmó la ilegitimidad de este

[14] STJUE, asunto C-746/18, párr. 51-53.
[15] STJUE, asunto C-746/18, párr. 54.
[16] Como se señala en el § 103 del Dictamen de Avv. gen. Pitruzzella de la UE.

marco normativo y la imposibilidad de postergar una reforma destinada a superar las fricciones con los estándares de garantía identificados por los jueces luxemburgueses[17]

El legislador ha intervenido finalmente con el art. 1 del Decreto-Ley 132/2021, de 30 de septiembre, ante la "extraordinaria necesidad y urgencia de garantizar la posibilidad de adquirir datos relativos al tráfico telefónico y electrónico a efectos de investigación penal de conformidad con los principios establecidos [...] en la sentencia de 2 de marzo de 2021»; decreto, posteriormente, convertido por la Ley 178/2021, de 23 noviembre.

Por lo que se refiere al momento de la adquisición, la nueva normativa marca la transición de un acceso centralizado e incondicional a todos los datos de tráfico almacenados por el operador, independientemente de los límites objetivos y teleológicos adecuados para limitar el citado acceso a lo estrictamente necesario; a un regime adquisitivo, delimitado ratione materiae y suficientemente preciso en cuanto a las condiciones específicas de la medida restrictiva. Con el fin de llegar a un equilibrio razonable entre los valores opuestos, a lo largo de las coordenadas marcadas por la reserva de ley y jurisdicción, así como por el canon de la proporción.

Desde el punto de vista de la competencia, de acuerdo tanto con el Derecho vigente de la Unión Europea como con el papel de parte procesal desempeñado por el fiscal en el sistema procesal penal italiano, este último se ha visto privado de legitimidad para ordenar la obtención de datos de tráfico; reservándola exclusivamente al Tribunal, como garante de los derechos fundamentales de la persona. Al reconocer la función de la acusación como un mero impulso, mediante una facultad de solicitud que se sitúa–de acuerdo con el principio de la acción dispositiva en materia de prueba-junto con la facultad de "petición del abogado del acusado, de la persona investigada, de la parte perjudicada y de otros particulares" (nuevo párrafo 3 del artículo 132 del Código de Privacidad 196/2003); o, en el momento de la validación posterior, "cuando existan razones de urgencia y existan razones razonables para creer que la demora puede resultar en un perjuicio grave para las investigaciones" (párrafo 3-bis).

La decisión de excluir los poderes de iniciativa de la acusación desvinculados del control directo del juez logra un mayor equilibrio entreel

[17] El 22 de julio de 2021 (doc web n. 9696764, in https://www.garanteprivacy.it), el Garante de la protección de datos personales instó inmediatamente a la necesidad de una reforma tras la sentencia *H.K. c. Prokuratuur*.

fiscal y los demás sujetos o partes que requieren adquisición dos datos. Sin embargo, todavía esiste algunos puntos de fricción con el principio de igualdad de las partes (artículo 111 de la Constitución italiana) en cuanto a los metodo concretos de ejecución del decreto sudicia que autoriza el acceso a los datos de tráfico[18].

Al llenar el vacío legal en cuanto a condiciones que legitiman la restricción del secreto sobre el hecho histórico de la comunicación y de manera similar a lo previsto para la interceptación de conversaciones o comunicaciones, el acceso a losdatos de la autoridad competente se ha vinculado a la doble condición sustantiva (la "prueba suficiente de un delito") y procesal (la pertinencia de los datos para la determinación de los delitos para los que la ley establece la pena de cadena perpetua o prisión no inferior a tres años, y de los delitos de amenza y hostigar o molestar a la persona por medio del teléfono), cuando la amenaza, el hostigamiento o la perturbación sean graves» (párrafo 3).

De este modo, como consecuencia de la referencia al concepto no técnico de prueba en sentido objetivo, para que el juez autorice legítimamente dicho acceso, es necesario disponer de elementos de prueba caracterizados por un grado «suficiente» de intensidad persuasiva y que puedan sugerir una relación pertinente entre los datos de tráfico obtenidos y la infracción penal. Por lo tanto, el acceso también puede implicar a usuarios (o computadoras) en nombre o en uso de sujetos completamente ajenos al delito por elque se está llevando a cabo el proceso, es decir, que no sean el sospechoso o acusado; siempre y cuando exista una conexión entre el usuario (o el ordenador) a controlar y el infractor. Esta solución normativa, similar a la ya prevista en materia de interceptación, tiene la ventaja de no excluirel uso de esta herramienta de vigilancia ex post en procedimientos contra personas desconocidas; al mismo tiempo, frenaría cualquier comportamiento elusivo –como el uso del teléfono o el ordenador de un amigo, que podría preverse si los datos del acusado estuvieran sujetos a un control a posteriori[19].

---

[18] En caso de negativa reiterada de los proveedores a cumplir la orden del juez, si bienel fiscal puede ordenar la incautación probatoria de los registros telefónicos, elabogado defensor de la persona interesada solo puede solicitar la intervención del juez. Críticas sobre este punto: Andolina Elena, "Acquisizione dei dati esterni", en *La nuova disciplina delle intercettazioni,* cur. por Maggio Paola (Torino: Giappichelli, 2023): 419; Dinacci Filippo, "L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia:luci europee e ombre legislative" (2021), in https://www.processopenaleegiustizia.it.

[19] Critica la decisión de someter también a control los servicios públicos de personas distintas del sospechoso/acusado, Filippi Leonardo, "La nuova disciplina dei tabulati: il commento "a caldo"(2021),

El citado informe de pertinencia es una condición sostantiva necesaria pero no suficiente para la accesibilidad a los datos, ya que no se desvincula de la ocurrencia de una finalidad procesal específica predeterminada por la ley, en vista de cuya satisfacción puede justificarse el impacto en la esfera individual. También debe existir un vínculo funcional, configurado en función de la «pertinencia» de la actividad de "adprehensio", entre los datos que deben obtenerse y la «determinación» del delito grave concreto por el que se está incoando el procedimiento.

La pertinencia de los datos de tráfico a efectos de la investigación permite la adquisición de tales datos no solo en los momentos posteriores al cierre de las investigaciones y a lo largo del juicio, sino también en las fases iniciales de la investigación como primer acto de investigación. La provisión de parámetros precisos a los que se basa la autorización para la adquisición de datos "externos" de tráfico telefónico implica un mayor rigor en el cumplimiento de la obligación de motivación adecuada y específica impuesta por la tasa de proporcionalidad y por el proprio artículo 15 de la Constitución italiana, como complemento de la reserva de jurisdicción y protección última del derecho inviolable al secreto contra el riesgo de injerencias arbitrarias e injustificadas.

Con ello se frena la lamentable tendencia –alimentada precisamente por el citado vacío normativo en cuanto a los supuestos de accesibilidad a los datos– de recurrir a razones aparentes, o pseudomotivaciones de contenido tautológico, que han acabado degradando, en la práctica, la obligación de motivación hasta el mero cumplimiento virtual.

En efecto, para cumplir con esta obligación, el juez deberá en el decreto de autorización no sólo indicar con suficiente claridad el título del delito para cuya comprobación pretende obtener los datos, sino también justificar las pruebas de lasque se deducen los indicios, así como las necesidades probatorias concretas que, en la práctica, se pretenden satisfacer con la citada adquisición.

Es claro, entonces, que la obligación de motivación se ve reforzada por la disposición expresa de la sanción estricta de la inutilización patológica, cuyo alcance se ha ampliado oportunamente a todos los "datos adquiridos en violación de las disposiciones de los párrafos 3 y 3-bis" por el nuevo párrafo 3-*quater,*artículo 132 del Código de Privacidad 196/2003.

---

en https://www.penaledp.it.

Por lo tanto, los datos adquiridos serán inutilizables no sólo en contraste con las garantías y métodos de adquisición a que se refieren los apartados 3 y 3-bis, sino también en ausencia de una justificación exhaustiva y articulada de la medida de adquisición.

En definitiva, resulta que el legislador, con vistas a la plena aplicación del principio de legalidad procesal también in subiecta materia, y respetando el principio de efectividad valorado por el Tribunal de Justicia, pretendía eliminar cualquier posible duda en cuanto a las consecuencias sancionadoras, optando expresamente –simétricamente– con las disposiciones sobre interceptación del art. 271, párrafo 1, código de procedimiento penal italiano – por la sanción severa de inutilización patológica. Una confirmación más de la importante capacidad intrusiva del instrumento en cuestiónes que, como tal, debe estar sujeta a mecanismos de protección homogéneos y, en todo caso, no menos garantistas que las previstas en el ámbito de la interceptación.

6. LA REFORMA DEL ART. 132 CÓDIGO DE PRIVACIDAD: SÓLO UNA ADAPTACIÓN PARCIAL A LA LEGISLACIÓN DE LA UE

La ley 178/2021 logra sin duda un cambio de rumbo en la dirección de las garantías, en línea con el sólido modelo de protección de la privacidad en lo que respecta a la protección de datos personales, implementado por el Tribunal de Justicia de la Unión Europea, pero solo limitado a la adquisición de datos "externos" de comunicaciones telefónicas y telemáticas con el fin de luchar contra la delincuencia grave. Es cierto que no sólo destaca la ubicación anómala fuera del código de procedimento penal del instrumento de investigación en cuestión[20], sino también el contraste del ius conditum con respecto al derecho de la Unión Europea en lo que respecta al aspecto específico de la conservación de datos («almacenamiento de datos»). Es innegable, en efecto, la evidente "asimetría" de la legislación interna debida tanto al exorbitante plazo de retención (párrafo 5-*bis* del artículo 132 del Código de Privacidad 196/2003), así como el regime sistemático e indiscriminado de archivo de todos los datos relativos al tráfico telefónico/telemático y a la localización, relativos a todos los

[20] A la luz de las afinidades con el instrumento interceptivo, reforzadas aúnmás por la sentencia *H.K. c. Prokuratuur*, la legislación pertinente debería haber encontrado su lugar natural en los medios de investigación y aseguramiento de la evidencia, inmediatamente después de la regulación de la captura de contenidos comunicativos.

abonados y/o usuarios(párrafos 1 y 1 *bis* del artículo 132).

Este último sigue siendo censurado por dos recientes sentencias del Tribunal de Justicia de la Unión Europea, que confirmaron la prohibición de la retención generalizada e indiscriminada de datos relativos al tráfico de comunicaciones electrónicas con el fin de luchar contra la delincuencia. Reiterando que la normativa nacional, para ser compatible con el art. 15, apartado 1, de la Directiva (UE) 2002/58 debe prever el almacenamiento selectivo de registros, delimitados sobre la base de pruebas objetivas, según categorías de personas afectadas, durante un período de tiempo limitado pero renovable[21].

Pero hay más. Tampoco es pienamente compatible el regime regulador de la adquisición "*a posteriori*" de datos "externos" de comunicaciones telefónicas o telemáticas con fines preventivos (artículo 226 de las disposiciones de coordinación del código de procedimiento penal italiano) con el sistema de protección previsto en los artículos 7, 8 y 52 de la Carta de los Derechos Fundamentales UE.

Las cuestiones más críticas siguen siendo la insuficiencia de las condiciones objetivas de la medida de autorización, así como la elección de conferir la legitimidad para ordenar la autorización de los controles preventivos, en lugar del juez, al fiscal («el fiscal del tribunal de la capital del distrito en el que se encuentra el sujeto a control o, si no es determinable, del distrito en el que han surgido las necesidades de prevención»)[22].

A la espera de la deseable armonización de toda la normativa sobre herramientas de vigilancia para la recogida automatizada de datos "externos" al contenido de la comunicación, queda confirmada la incompatibilidad con el Derecho de la Unión y la consiguiente "precariedad" del sistema normativo interno en lo que respecta a los perfiles de fricción aún no superados por el legislador. De hecho, no está demás recordar que es una obligación de los

[21] Tribunal de Justicia de la Unión Europea. Sentencia de 20 de septiembre de 2022, asuntos VD (C-339/2020) e SR (C-397/20), y SR (C-397/20), y sentencia de 5 de abril de 2022, *G.D. c. Commissioner of the Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General*, asunto C-140/20. Sobre las consecuencias de esta última sentencia en el derecho italiano, Iovene Francesca, "Nuova decisione della Corte di Giustizia in materia di tabulati: quali conseguenze per l'ordinamento nazionale?", in *Cassazione penale* 6 (2022): 2344.

[22] Del mismo modo, la competenciaconcurrente del Fiscal General del Tribunal de Apelación de Roma para autorizar, de conformidad con el art. 4, párr. 2, del Decreto Legislativo n.º 144/2005, los controles preventivos contra el terrorismo y la subversión exigidos por los directores de los servicios de inteligencia de seguridad (controles de seguridad).

órganos jurisdiccionales nacionales, sobre la base de la primacía del Derecho europeo, «garantizar la plena eficacia de [esta última] mediante la inaplicación, en su caso, por propia iniciativa, de cualquier disposición contraria de la legislación nacional, aunque sea posteriormente, sin tener que solicitar o esperar a su supresión previa por vía legislativa o constitucional»[23].

REFERENCIAS BIBLIOGRÁFICAS

A Amato Giuseppe, *Nella "costruzione"normativa si è sminuito il ruolo del p.m.,* in *Guida diritto* nº 39 (2021), de 16 octubre.

Andolina Elena, *Acquisizione dei dati esterni*, in *La nuova disciplina delle intercettazioni,* curado por Maggio Paola, (Torino: Giappichelli, 2023): 402.

Ead., *La sentenza della Corte di giustizia UE nel caso H.K. c. Prokuratuur: un punto di non ritorno nella lunga querelle in materia di data retention?*, in www.processopenaleegiustizia.it (2021).

Ead., *L'acquisizione nel processo penale dei dati esteriori delle comunicazioni telefoniche e telematiche*, (Milano: Cedam, 2018).

Aprile Ercole, Spiezia Filippo, *Le intercettazioni telefoniche e ambientali. Innovazioni tecnologiche e nuove questioni giuridiche,* (Milano: Giuffrè, 2004).

Baccari Gian Marco., *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati,* en *Cybercrime,* dirigido por Cadoppi Alberto, Canestrari Stefano, Manna Alberto y Papa Michele (Milano: Utet Giuridica, 2019): 1868.

Bertuol Roberto, *La nuova disciplina per l'acquisizione dei tabulati telefonici: l'interpretazione "autentica" del legislatore e la parola fine alla (fin troppo) lunga* querelle *giurisprudenziale*, en *Giurisprudenza penale* (2021): 12.

Caianello Michele, *Il principio di proporzionalità nel processo penale*, en http://archiviodpc.dirittopenaleuomo.org (2014).

Camon Alberto, *L'acquisizione dei dati sul traffico delle comunicazioni*, en *Rivista italiana di diritto e procedura penale* (2005): 594.

Cisterna Alberto, *Cedu e diritto alla* privacy, en *Principi europei del processo penale*, curado por Gaito Alfredo, (Roma: Dike Giuridica, 2016), 193.

Costanzi Claudio, Big data *e garantismo digitale. Le nuove frontiere della giustizia penale nel XXI secolo, e*n *www.lalegislazionepenale.ue* (2019).

De Leo Francesco, *Controllo delle comunicazioni e riservatezza (a proposito di tabulati, tracciamenti, intercettazioni, conservazione dei dati e dintorni)*, en *Cassazione*

[23] STJUE, asunto C-140/20.

penale, nº 42 (2002): 2208.

Demartis Fabrizio, *La nuova disciplina sui tabulati: un completo adeguamento agli standard europei?,* en *Diritto penale e processo,*nº 3 (2022): 299.

Dinacci Filippo, *L'acquisizione dei tabulati telefonici tra anamnesi, diagnosi e terapia: luci europee e ombre legislative,* en www.processopenaleegiustizia.it (2022).

Filippi Leonardo, *La nuova disciplina dei tabulati: il commento "a caldo"*, en in https://www.penaledp.it.(2021).

Id., *Intercettazioni, tabulati e altre limitazioni della segretezza delle comunicazioni, Soggetti, atti e prove,* vol. I, *Procedura penale. Teoria e pratica del processo,* dirigido por Spangher Giorgio, (Torino: Utet Giuridica, 2015): 1100.

Galgani Benedetta, *Giudizio penale,* habeas data *e garanzie fondamentali*, en www.archiviopenale.web (2019).

Iovene Federica, *Nuova decisione della Corte di Giustizia in materia di tabulati: quali conseguenze per l'ordinamento nazionale, e*n *Cassazione penale,* nº6 (2022): 2363.

Lorusso Sergio, Digital evidence, cyber crime *e giustizia penale*, en www.processopenaleegiustizia.it (2019).

Marcolini Stefano, *L'istituto della* data retention *dopo la sentenza della Corte di giustizia del 2014, e*n *Cybercrime,* dirigido por Cadoppi Alberto, Canestrari Stefano, Manna Alberto y Papa Michele (Milano: Utet Giuridica, 2019): 1849.

Natalini Aldo, *Relazione n. 55/2021 del Massimario sulle novità introdotte dal d.l. 132/2021 in tema di acquisizione di tabulati telefonici e telematici,* en https://www.sistemapenale.it (2021).

Rodotà Stefano, *Prefazione*, *Libera circolazione e protezione dei dati personali*, curado por Panetta Rocco, (Milano: Giuffrè, 2006).

Signorato Silvia*, Le indagini digitali. Profili strutturali di una metamorfosi investigativa,* (Torino: Giappichelli, 2018).

Spangher Giorgio, Data retention: *svolta garantista ma occorre completare l'impianto, e*n *Guida diritto* (2021), nº 39, de 16 octubre.

ELENA AUGUSTA ANDOLINA
Università degli Studi "Magna Graecia" de Catanzaro (Italia), Dipartimento di Giurisprudenza, Economia e Sociologia
elena.andolina@unicz.it
Orcid: 0009-0009-0680-8055