Revista Vasca de Derecho Procesal y Arbitraje

Dirección
Prof. Dr. Dr. Dr. h. c. mult. Antonio María Lorca Navarrete

Contenido / Contents

Universidad del País Vasco Euskal Herriko Unibertsitatea

Da mihi factum dabo tibi ius
INSTITUTO VASCO DE DERECHO PROCESAL

1
2024

TOMO XXXVI

PREMIOS 2023 INSTITUTO VASCO DE DERECHO PROCESAL
AWARDS 2022-2023 BASQUE INSTITUTE OF PROCEDURAL LAW

CONTENIDO / CONTENTS

CESIÓN DE DATOS COMERCIALES RELATIVOS A LAS COMUNICACIONES PARA FINES DE INVESTIGACIÓN CRIMINAL[*]

José Luis Rodríguez Laín[**]
Córdoba

* * *

Es evidente que habría que sacrificar cierto grado
de libertad en beneficio de la justicia y
cierto grado de justicia en beneficio de la libertad".
(BERTRAND RUSSEL. Prólogo a la Tercera Edición,
versión en inglés, de *"Los caminos de la Libertad"*, junio de 1948)

I- EL ORIGEN: LOS DATOS RELATIVOS A LAS COMUNICACIONES ELECTRÓ-

---

[*] El trabajo ha obtenido el Premio Instituto Vasco de Derecho Procesal en su XIII Edición del año 2023.
[**] José Luis Rodríguez Laín es Magistrado titular del juzgado de Instrucción 4 de Córdoba.

TRÓNICAS COMO FUENTE DE INVESTIGACIÓN CRIMINAL[1]

Todo comenzó cuando en agosto de 1984 el Tribunal Europeo de Derechos Humanos –TEDH- hubo de enfrentarse por primera vez a una realidad tecnológica que permitía sacar cierto partido a la investigación criminal a través del análisis de datos de tráfico de comunicaciones ya consumadas, y no necesariamente objeto de previo seguimiento en tiempo real. Del rudimento del *comptage* o *metering*, bien en base a la capacidad innata de ciertos funcionarios policiales para calcular mentalmente el tiempo que tardaba el dial de un teléfono intervenido en retornar al punto de reposo, bien al empleo de herramientas mecánicas que sustituían a aquéllos de una forma más fiable[2], se había pasado a la comodidad de poder solicitar al correspondiente prestador del servicio de telefonía una información detallada sobre cuestiones tan relevantes como números de abonado con el que un determinado terminal telefónico hubiera contactado, tanto como emitente como receptor, en un determinado período de tiempo, datación y duración de la llamada.

La STEDH de 4 de agosto de 1984 (caso MALONE v. Reino Unido, asunto 8691/79) asumió este reto, enfrentándose a un supuesto de hecho en el que el Sr. Malone imputaba a las autoridades policiales británicas haber accedido durante años a información detallada sobre sus contactos telefónicos; siendo una de las posibilidades técnicas para que ello hubiera podido tener lugar, al haberse negado por las autoridades británicas la existencia de más interceptaciones que las correspondientes a un breve período de tiempo, precisamente la de acudir al prestador de telecomunicaciones para que facilitara dicha información almacenada por éste por razones comerciales.

Sin perjuicio de realizar la comprometida afirmación de que el examen, tras su cesión, de la información referida a lo que en el futuro fueran definidos como datos de tráfico, aunque de diferente naturaleza, comportaba una afectación del derecho al respeto de la correspondencia, garantido como tal por el art. 8.1 del Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales, de 4 de noviembre de 1950 –CEDH-[3], el Alto Tribunal Europeo concluirá realizando una importante aportación sobre la conformidad con dicho precepto de las prácticas de las operadoras de telecomunicaciones de conservar y tratar tales datos, en tanto en cuanto ello fuera preciso para la prestación del ser-

[1] El presente trabajo forma parte del Proyecto PID2022-137826NB-I00 financiado por el Ministerio de Ciencia e Innovación-Agencia Estatal de Investigación sobre *"Datos personales e información en la era digital: desafíos en su obtención y uso en los procesos judiciales y en los procedimientos sancionadores (DATER)"*.

[2] El *meter check printer* era un dispositivo empleado por las autoridades policiales británicas para descubrir los contactos telefónicos de un determinado terminal objeto de interceptación legal. El dispositivo no solo permitía identificar de forma mecánica los números de teléfono marcados por el dispositivo, sino también fecha y duración de las llamadas. Véase sobre el particular el § 56 de la STEDH de 4 de agosto de 1984 (caso MALONE v. Reino Unido; asunto 8691/79).

[3] *"The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8 (art. 8). The records of metering contain information, in particular the numbers dialed, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8".*

vicio –§ 84-[4]. Era legítimo, por tanto, que las operadoras trataran estos datos a los efectos de dar respuesta a las finalidades legítimas de su captación y conservación; no pudiendo negarse, en consecuencia, como sucediera en el precedente de la sentencia del caso MALONE v. Reino Unido, que las autoridades competentes pudieran recabar tal información de aquéllas en el contexto de una investigación criminal, en tanto que la decisión pudiera tener cabida dentro del margen de actuación que determinara el apartado 2 de dicho precepto del CEDH.

Ya dentro del universo de las comunicaciones electrónicas, el mismo planteamiento sería reproducido, entre otras, diecisiete años después, por la STEDH, Secc. 3ª, de 25 de septiembre de 2001 (caso P.G. y J.H. v. Reino Unido; asunto 44787/98)[5]. La idea de que las operadoras de comunicaciones electrónicas estarían legitimadas para el almacenamiento y tratamiento de estos datos, siempre siguiendo un referente de finalidad o funcionalidad, y que la información así tratada pudiera tener acceso a una investigación criminal, encontraba un firme sustento en la jurisprudencia del TEDH. Solamente en supuestos en los que la fuente de conocimiento tuviera un origen diverso a la prestación de un servicio de telecomunicaciones, y pudiera esgrimirse por el usuario afectado por la injerencia una situación de expectativa razonable de privacidad, especialmente en el ámbito de las relaciones laborales, este posible almacenamiento y uso sí podría confrontarnos con una transgresión del art. 8.1 del CEDH; tal y como nos indicaran las célebres SSTEDH, Secc. 4º, de 3 de abril de 2007 (caso COPLAND v. Reino Unido; asunto 62617/00), y, Gran Sala, de 5 de septiembre de 2017 (caso BĂRBULESCU v. Rumanía, 61496/08).

El análisis de los datos que son tratados y conservados por las operadoras de comunicaciones electrónicas o prestadores de servicios de la sociedad de la información, que tienen por objeto canalizar el intercambio de información entre personas, ha adquirido de manera cada vez más creciente un importantísimo papel en la investigación criminal. La interceptación de comunicaciones en tiempo real presupone la identificación del sospechoso y el encauzamiento de una investigación concreta contra éste y por supuesta infracción criminal, con propensión de expandir su propia dinámica o efectos en el futuro, solamente atañe a un número muy limitado de supuestos. La investigación criminal es, casi por definición, un proceso de indagación que afecta a hechos del pasado; y ello no hace sino reproducirse de forma muy marcada en la investigación de hechos ya acontecidos, bien en un escenario tecnológico, bien en un escenario real, pero que permiten ser esclarecidos gracias a un adentramiento en una realidad tecnológica como fuente de obtención de evidencias. Podemos identificar al autor de una estafa por Internet si descubrimos la IP que le fuera asignada al colgar en un popular portal de anuncios una oferta falsa de alquiler de un apartamento vacacional en Benidorm; o facilitar la identidad del autor de un brutal atentado terrorista en un tren de cercanías gracias al recabo de información sobre los IMSI de terminales telefónicos móviles bajo la cobertura de una estación de telefonía móvil tipo BTS en determinada franja de tiempo. En ambos supuestos la colaboración del prestador que almacenara legítimamente dichos datos sería tanto o más importante que una posible interceptación de comunicaciones que partiría de su imposible anticipación.

II. EL ESCENARIO DEL DERECHO DE LA UNIÓN EUROPEA

[4] *"As the Government rightly suggested, a meter check printer registers information that a supplier of a telephone service may in principle legitimately obtain, notably in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service".*

[5] En igual sentido se pronunciará la STC 123/2002, de 20 de mayo.

La Directiva 95/46/CE[6] representaría la definitiva apuesta del legislador comunitario por someter a regulación el complejo y cambiante ámbito regulatorio de la protección de datos de carácter personal. Si el TEDH analizó la legitimidad del almacenamiento y tratamiento de datos relacionados con telecomunicaciones en un contexto de funcionalidad, la Directiva 95/46/CE, frente al precedente del Convenio Europeo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal de 1981, avanzará no solo reconociendo la trascendencia del principio del consentimiento al tratamiento, sino su clara preponderancia. Así se podía apreciar de la lectura de su art. 7; colocando en primer lugar al consentimiento del interesado entre los criterios que legitiman al tratamiento de datos. Por supuesto que ese criterio de funcionalidad anticipado por la jurisprudencia del TEDH encontraría igualmente un reconocimiento en el apartado b) del mismo precepto; pero esa evidente preponderancia del principio del consentimiento marcaría claramente toda la estructura de la norma comunitaria. El tratamiento de datos relativos a las comunicaciones no era considerado en modo alguno como una excepción. Además, el art. 13 desarrollaba un régimen jurídico que permitía excepcionar el ejercicio de determinados derechos de los ciudadanos relacionados con la protección de sus datos personales en razón de un interés público superior; entre los que se encontraba *"la prevención, la detección y la represión de infracciones penales"* -art. 13.1,d)-.

Pronto el legislador comunitario fue consciente de la urgencia de abordar el tratamiento de datos relacionados con comunicaciones electrónicas como una especialidad frente a dicha normativa[7]. Tráfico internacional de datos, constante evolución de las tecnologías de las comunicaciones y potencialidad de afectación de derechos fundamentales de los usuarios consecuencia de la necesaria intermediación de prestadores de servicios de comunicaciones electrónicas, estaban detrás de esta necesaria revolución normativa. Es en este contexto donde surgirá una norma, la Directiva 2002/58/CE[8], con vocación de regular la protección de datos en el ámbito de las comunicaciones electrónicas; haciéndolo, además, con el claro cometido de convertir el criterio de funcionalidad en el almacenamiento y tratamiento de datos en prevalente, frente a un consentimiento que pasaba a ser auténticamente gregario de aquél.

Uno de los cometidos esenciales de la Directiva, nos dirá su art. 5.1, sería el de garantizar *"…la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público"*; aunque para ello el mismo precepto se mostrara comprensivo de la necesidad del tratamiento técnico de los datos de tráfico por parte de los prestadores de servicios, sometidos a un mismo principio de confidencialidad común a los contenidos de comunicaciones[9]. Y es de aquí de donde parte la norma para desarrollar en sus

[6] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.

[7] El art. 1.2 de la Directiva 2002/58/CE, a la que seguidamente haremos mención, sentará con claridad esta naturaleza especial de la norma en relación con el tronco común de la Directiva 95/46/CE. Establecía, de hecho, que: *"Las disposiciones de la presente Directiva especifican y completan la Directiva 95/46/CE a los efectos mencionados en el apartado 1…".*

[8] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

[9] *"El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad".*

arts. 6 y 9 ese marcado principio de funcionalidad que llega a lastrar severamente cualquier posibilidad de obtener del usuario un consentimiento lícito a un tratamiento más allá de las necesidades propias de la prestación del servicio demandado.

El tratamiento de los datos de tráfico –art. 6-, comienza con un incontestable sometimiento a ese principio de funcionalidad; de suerte que la regla general será la de que solamente se permita el tratamiento de datos de tráfico generados por las comunicaciones mantenidas por abonados y usuarios en tanto ello fuera preciso para la transmisión de una comunicación. A partir de la pérdida de esa funcionalidad, nos dirá el apartado 1 de dicho precepto, el destino de los datos no podría ser otro que el de su destrucción o anonimización. Ahora bien, la propia norma intenta relajar tan estricta limitación; definiendo otras situaciones en las que, bien por las necesidades propias de la relación contractual, bien por abrirse a la posibilidad de cierta condescendencia con la irrupción del principio del consentimiento, se desvanecerá el nudo criterio de la estricta funcionalidad a los efectos de canalización de una concreta comunicación. Por una parte, determinados datos de tráfico habrían de poder ser conservados en tanto en cuanto ello fuere preciso a los efectos de *"…la facturación de los abonados y los pagos de las interconexiones"*; lo que permitiría su almacenamiento y tratamiento al menos hasta el momento en que expirara el plazo durante el cual pudiera legalmente impugnarse la factura o exigirse el pago[10]. Promoción comercial y prestación de servicios de valor añadido[11]

[10] Determinar realmente cuáles son estos plazos tanto de reclamaciones por parte de los abonados como de posible ejercicio de acciones de cobro de facturas impagadas nos enfrenta a un complejo dilema jurídico. El art. 27 del Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas, es la norma que en un principio disciplinaría el cauce de reclamación de los abonados frente a decisiones de operadoras de telecomunicaciones; entre las que sin duda estaría la reclamación frente a facturas emitidas. La norma presupone un previo procedimiento de reclamación directa ante los servicios de atención al cliente de la propia operadora; en un contexto en el que cada Comunidad Autónoma, en el ejercicio de sus competencias propias en materia de consumo, podría establecer procedimientos específicos de resolución de controversias. Realmente, solo se regula un trámite administrativo de reclamación ante la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información; en el que intervendría como órgano con capacidad de resolución la División de Atención al Usuario de Telecomunicaciones -art- 8.3 del Real Decreto 1554/2004, de 25 de junio, por el que se desarrolla la estructura orgánica básica del Ministerio de Industria, Turismo y Comercio-. El apartado 2 de dicho art. 27, sin perjuicio de prever la aprobación de una Orden Ministerial que regulará el procedimiento, aún no aprobada, establece un plazo único de seis meses para resolver y notificar la resolución. Sí existe una Orden Ministerial preexistente al referido RD 899/2009; y que, a falta de desarrollo de dicho mandato reglamentario, deberíamos considerarla en vigor: la Orden ITC/1030/2007. Al menos en aquellas Comunidades Autónomas en que no se hubiera desarrollado una normativa propia debería ser considerada ésta como norma aplicable. En ella se establece un procedimiento previo de reclamación para finalidades concretas desarrolladas en su art. 3 (prácticamente todos los ámbitos imaginables, a excepción de reclamación de indemnizaciones por fallos del servicio o impugnación de cláusulas que pudieran considerarse por el abonado abusivas); y se marca como plazo para la reclamación el de un mes *"…desde el momento en que se tenga conocimiento del hecho que motiva la reclamación"*; que abriría un plazo de otro mes para recibir la respuesta de la operadora o para abrir el camino a la reclamación en sede administrativa. Ello, como podemos fácilmente apreciar, supone un solapamiento de plazos que dificulta seriamente la determinación concreta de unos plazos de legítima conservación, difícilmente conciliables con una legislación administrativa en materia de sentido del silencio por no respeto de los plazos de resolución que no está pensada para solventar conflictos jurídicos entre particulares; y que, además, no debería cerrar definitivamente las puertas para que un ciudadano, insatisfecho ante la respuesta de su operadora de telecomunicaciones ante una reclamación sobre facturación, pudiera acudir a la jurisdicción civil, con evidentes lagunas jurídicas sobre cuál sería en tal supuesto el momento del inicio del cómputo del