INFORMÁTICA Y DERECHO

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – N.º 13, 2023, PP. 119-132

LA ORDEN DE CONSERVACIÓN DE DATOS: UNA MEDIDA DE ASEGURAMIENTO DE FUENTES DE PRUEBA IMPRESCINDIBLE PARA LA INVESTIGACIÓN DE LOS DELITOS DE ODIO COMETIDOS EN LÍNEA

THE DATA PRESERVATION ORDER: AN ESSENTIAL MEASURE TO SECURE SOURCES OF EVIDENCE FOR THE INVESTIGATION OF HATE CRIMES COMMITTED ONLINE

Juan Alejandro Montoro Sánchez[1]

Investigador Posdoctoral Margarita Salas. Universidad Pablo de Olavide de Sevilla

1 Trabajo vinculado al Proyecto de Investigación de Excelencia del Ministerio de Economía y competitividad «Límites a la utilización de datos, evidencias e información entre procesos y procedimientos diversos en España y la Unión Europea (LUDEI)». Esta publicación ha sido financiada por la Unión Europea "NextGenerationEU", por el Plan de Recuperación, Transformación y Resiliencia y por el Ministerio de Universidades, en el marco de las ayudas Margarita Salas, para la Recualificación del sistema universitario español 2021-2023 convocadas por la Universidad Pablo de Olavide, de Sevilla

Resumen

El presente trabajo aborda el estudio de la regulación de la orden de conservación de datos prevista en el art. 588 octies *LECrim*, como medida idónea de aseguramiento de fuentes de prueba a disposición de la Policía Judicial y del Ministerio Fiscal para garantizar la eficacia de la investigación de los delitos de odio cometidos en línea.

Palabras clave

Ciberdelitos de odio, orden conservación datos, investigación del delito.

Abstract

This paper studies the regulation of the data preservation order provided for in art. 588 octies LECrim, as a suitable measure for securing sources of evidence at the disposal of the Judicial Police and the Public Prosecutor's Office to guarantee the effectiveness of the investigation of hate crimes committed online.

Keywords

Cyber hate crime; data preservation order; crime investigation.

Los delitos de odio cometidos en línea: un preocupante fenómeno creciente

La Organización para la Seguridad y la Cooperación en Europa, como institución encargada de supervisar los delitos de odio y la incitación al odio, define a éstos como cualquier infracción penal donde la víctima, el local o el objetivo de la infracción se elija por su (real o percibida) conexión, simpatía, filiación, apoyo o pertenencia a un grupo basado en una característica común de sus miembros, como su raza real o perceptiva, el origen nacional o étnico, el lenguaje, el color, la religión, el sexo, la edad, la discapacidad intelectual o física, la orientación sexual u otro factor similar[2]. En nuestro Código Penal, son diversas las modalidades de tipos delictivos los que pueden ser calificados como auténticos delitos de odio, constituyéndose el art. 510 CP (Código Penal) como el principal de éstos, sin perjuicio de que asimismo puedan considerase como tales los catalogados en los arts. 170.1; 173.1; 174; 314; 511 y 512; 515.4 y 522 a 525 del mismo texto legal.

De acuerdo con las últimas estadísticas publicadas por la Oficina Nacional de Lucha contra los Delitos de Odio en el "Informe de la Evolución de los Delitos de Odio en España" correspondiente al ejercicio 2021[3], se contabilizaron en éste un total de 1802 hechos delictivos de odio por las Fuerzas y Cuerpos de Seguridad del Estado, bien por mediar la interposición de una denuncia, bien por tener constancia durante el desarrollo de sus labores propias. Esta cifra, que en términos absolutos puede parecer reducida, supone un nada desdeñable incremento del 28,62 % de los delitos conocidos en el año anterior, en el que se contabilizaron un total de 1401[4]. En cualquier caso, es imprescindible apuntar que esta cifra solo representa la punta del iceberg de la situación real, ya que se considera que la mayor parte de los delitos de esta índole que se cometen no se llegan a conocer oficialmente, lo que impide la inclusión en las estadísticas oficiales[5]. De hecho, la

2 Esta es la definición utilizada por la OSCE en sus informes sobre los delitos de odio motivados por el racismo y la xenofobia (2021), los delitos de odio por motivos de género (2021), los delitos de odio por motivos de antisemitismo (2019) y los delitos de odio por motivos de islamofobia (2018), basados en la Decisión n.º 9/09 del Consejo Ministerial de la OSCE, de 2 de diciembre de 2009, sobre la lucha contra los delitos de odio, acordada por consenso por todos los Estados de la OSCE, incluidos todos los Estados miembros de la UE.

3 Disponible en https://www.fiscal.es/memorias/memoria2021/FISCALIA_SITE/index.html. (Fecha de consulta 15 de enero de 2023)

4 La Memoria de la Fiscalía General del Estado de 2019 ya era consciente tales incrementos, que se vienen repitiendo con más intensidad desde entonces y afirma incluso que "Si en la Memoria del año pasado comenzábamos haciendo referencia a un incremento de los denominados delitos de odio, tanto de las agresiones por motivos racistas, xenófobos, antigitanos, homófobos y otras formas de intolerancia y discriminación, como del discurso de odio en internet y las redes sociales, ahora podemos decir que no hay un día en que los medios de comunicación no relaten hechos que, con mayor o menor fortuna, entienden ser delitos de odio". Disponible en https://www.fiscal.es/memorias/memoria2019/FISCALIA_SITE/index.html. (Fecha de consulta 15 de enero de 2023).

5 TAMARIT SUMALLA, J. M., "Los delitos de odio en las redes sociales", *Revista de Internet, Derecho y Política*, núm. 27, 2018, p. 18.

Agencia Europea de Derechos Fundamentales estima que el 80 % de los delitos de odio no son denunciados por las víctimas y, por tanto, no llegan a conocerse[6].

En el mismo informe elaborado por la Oficina Nacional de Lucha contra los Delitos de Odio se informa que un total de 232 de todos los delitos de odio de los que se tuvo constancia en 2021 fueron cometidos a través de las TIC (Tecnologías de la Información y Comunicación) o valiéndose de instrumentos tecnológicos, siendo los delitos vinculados a la ideología, racismo, orientación sexual e identidad de género los que presentan una mayor incidencia en este concreto ámbito[7]. Este dato representa un porcentaje del 16,55 % respecto al total de los delitos de esta naturaleza, lo que supone, a su vez, un nada desdeñable incremento del 22,75 % respecto al ejercicio anterior, dato que evidencia una notoria tendencia alcista de esta vía comisiva. Cifras, ambas, que por ser muy significativas han merecido la preocupación de diversas instituciones implicadas en la lucha contra esta lacra. Por ejemplo, la Fiscalía General del Estado en su Memoria correspondiente al ejercicio 2018 ya advertía de esta creciente problemática por las facilidades que ofrecen las TICS para publicitar contenidos relativos al discurso del odio o para permitir la comisión de estas modalidades delictivas[8], de las que se deriva un incuestionable y perverso efecto sobre los valores y principios que inspiran nuestro modelo de convivencia[9]. Mientras en la más reciente Memoria de la FGE de 2021, elaborada una vez superada la pandemia por COVID19, se menciona que dado que las actividades de todo orden que desarrollan los ciudadanos se vieron intensamente limitadas y la interacción social fuertemente restringida, particularmente durante la vigencia de las medidas más estrictas de confinamiento, buena parte de las relaciones entre las personas y los grupos sociales se desarrollaron no de forma directa y personal sino a través de las TIC y redes sociales, factor que propició un aumento de los delitos de odio producidos a través de las tecnologías digitales de la información y la comunicación[10].

6 Se recomienda la lectura del apartado 12.7 de las Estadísticas de la Memoria anual de la Fiscalía General del Estado del año 2019, en el que se ponen de manifiesto algunos de los factores adicionales que impiden ofrecer una cifra más realista de las estadísticas en esta materia. De hecho, se enfatiza en la existencia de un problema estadístico sobre estos delitos que impide la obtención de una visión realista de su alcance en la sociedad.

7 Adviértase nuevamente que estas cifras no revelan la realidad. La Memoria FGE de 2019 se hace eco del hecho de que las redes e internet se encuentran llenas de mensajes de odio y de incitación al odio, unos más o menos espontáneos, otros muy organizados, sin embargo la estadística no depende tanto de su número tanto como de las denuncias y del rastreo que se pueda hacer en las redes por las Fuerzas y Cuerpos de Seguridad del Estado o la Administración.

8 Con anterioridad, la Memoria de la FGE de 2017 ya recogió un incremento de las denuncias por delitos de odio a través de internet y las redes sociales, pasando de 40 en 2015 a 99 en 2016. Disponible en https://www.fiscal.es/memorias/memoria2017/FISCALIA_SITE/index.html. (Fecha de consulta 15 de enero de 2023).

9 Pues como ya advirtió el Tribunal Supremo en su STS de 4 de mayo de 2015, "los valores de antirracismo o la tolerancia ideológica y religiosa son esenciales de la convivencia…".

10 Disponible en https://www.fiscal.es/memorias/memoria2021/FISCALIA_SITE/index.html. (Fecha de consulta 15 de enero de 2023).

Del total de los 232 delitos de odio denunciados en 2021 que se produjeron por vía telemática, un 37,83 % se cometieron a través de internet mediante publicaciones insertadas en páginas webs, blogs o foros. El 22,29 % de las denuncias se referían a publicaciones vertidas o mensajes proferidos en cualquiera de las distintas y numerosas redes sociales existentes. Con una cifra muy cercana a la anterior, esto es, con un 25,22 % se posicionarían los delitos de odio cometidos a través de vía telefónica, categoría que aglutina a los ilícitos cometidos mediante llamadas telefónicas o bien valiéndose de la mensajería tradicional (SMS, MMS) o de la instantánea a través de alguna de las distintas aplicaciones OTP que permiten este tipo de comunicación. Y en último lugar, con un 5,28 % de incidencia, se encontrarían los delitos cometidos a través de medios de comunicación, esto es, a través de publicaciones localizadas en diarios, rotativos y revistas que presentan una edición digital.

Vistos los anteriores datos, puede concluirse sin temor a duda que las tecnologías de la información y comunicación se han convertido tanto en un instrumento, como en un medio habitual para la comisión de acciones delictivas vinculadas al discurso del odio en cualquiera de las diferentes modalidades que encuentran acomodo en el código Penal. La facilidad de acceso a los medios tecnológicos y la sencillez de publicación de contenido en la red, el aparente anonimato que posibilitan estos medios, la desinhibición con la que los usuarios actúan y el desarrollo de identidades disociativas son factores que favorecen y propician que en estos canales se produzca la difusión o emisión de contenidos que incitan al odio, a la violencia o la discriminación respecto de individuos que son diferentes por su raza, religión, nacionalidad, sexo, orientación sexual, enfermedad o por su mera ideología[11].

Estas circunstancias no resultan baladíes para el desarrollo de las labores de investigación llevadas a cabo por las autoridades públicas competentes dirigidas al esclarecimiento de los hechos delictivos y la determinación de sus verdaderos, con miras al posterior ejercicio del *ius puniendi*. De hecho, lo cierto es que la utilización de estas vías comisorias condiciona sobremanera las técnicas y medidas que las autoridades deben emplear para la obtención exitosa del material probatorio requerido para la acreditación de los hechos tipificados. Pero muy especialmente, estos cada vez más habituales canales delictivos influyen en el tiempo de reacción que se precisa para la práctica de las primeras diligencias destinadas a recolectar los efectos del delito y las fuentes de prueba pertinentes, puesto que un grado notable de la eficacia de los iniciales actos de prevención o investigación va a depender de la inmediatez con la que se ejecuten tras el momento de la comisión del delito o, en su caso, de la toma de conocimiento de la *notitia criminis*. Piénsese que la información y los datos electrónicos que se albergan en la red, y particularmente aquellos que se generan voluntariamente en ciertos espacios de encuentro, redes sociales o aplicaciones de comunicación se caracterizan precisamente no ya por la facilidad con que pueden alterarse, si no por la extremada sencillez con la que pueden ser objeto de supresión o incluso

11 GONZÁLEZ JIMÉNEZ, A., "Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes", *Revista de Internet, Derecho y Política*, núm. 27, p. 19.

destrucción[12]. Tan sencillo y rápido es publicar un comentario de odio dirigido a una persona o colectivo en una multitudinaria red social, a través de una entrada de blog o en una revista digital como proceder a su inmediato borrado, eliminando cualquier huella aparente de su previa existencia. De hecho, la doctrina ha destacado a la volatilidad como una de las notas características e inherentes que presenta la información de carácter electrónico[13].

Por tanto, en los supuestos en los que produzca la interposición de una denuncia por la comisión de delito de odio a través de la publicación de contenido ofensivo en la red, es esencial que las primeras diligencias de investigación destinadas a la obtención de rastros y evidencias se desarrollen de forma apresurada y ágil, a fin de sortear los riesgos de alteración o supresión que acechan y que podrían dificultar, *a priori* y sin perjuicio de que se desarrollen otras diligencias más complejas, la constatación del delito. Asimismo, hay que advertir, que tales riesgos no dependen exclusivamente de la voluntad del sujeto responsable, si no que pueden tener origen, incluso, en la propia actividad del titular del medio o canal electrónico en el que se incorpore el contenido ofensivo. Por ejemplo, piénsese en aquellos supuestos en que medie una denuncia interna de la propia víctima o de otros usuarios que han tenido acceso al contenido ilícito y el proveedor del sitio web procede a eliminar o restringir el acceso para minimizar sus efectos lesivos y evitar cualquier tipo de responsabilidad como prestador, según las disposiciones establecidas en los arts. 10 y siguientes de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Ahora bien, debe tenerse en cuenta que gran parte de la investigación de estos delitos comienza por la denuncia que se interpone en dependencias policiales. Sin embargo, la solicitud o requerimiento de entrega de datos e información a los prestadores de servicios de comunicaciones electrónicas o de la sociedad de información, en tanto titulares de las plataformas o redes sociales en las que se almacenan y desde las que se difunden las manifestaciones y declaraciones de odio, requiere ineludiblemente de la pertinente autorización judicial dada la consecuente injerencia en ciertos derechos fundamentales de los individuos titulares de la información, como por ejemplo, en los derechos a la intimidad personal o a la protección de datos. Piénsese, por ejemplo, en los datos electrónicos conservados por los prestadores de servicios en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa con fines comerciales o, los datos almacenados en servidores y equipos, cuya entrega requiere preceptivamente la respectiva autorización judicial

12 La STS 300/2015, de 19 de mayo afirma que "la posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas". No obstante, a pesar de esta mutabilidad, lo cierto es que como contrapartida, la información digital o electrónica también se caracteriza por su trazabilidad, es decir, por la posibilidad de rastrear la huella de la misma a través de los registros que se generan y conservan en los sistemas informáticos por razón de su uso.

13 Por ejemplo, DELGADO MARTÍN señala que "la prueba electrónica ostenta frecuentemente la característica de la volatilidad, es decir, la información o datos relevantes son mudables y sometidos a constante cambio, especialmente en relación con los contenidos de Internet". DELGADO MARTÍN, J., "La prueba electrónica en el proceso penal", *Diario La Ley*, núm. 8167, 2013.

de conformidad con lo dispuesto en los arts. 588 *ter* j) y 588 *septies* a) LECrim. En consecuencia, los agentes de la Policía Judicial no están facultados en la mayoría de los supuestos, para solicitar y requerir coercitivamente, por sí mismos, a los proveedores de servicios electrónicos a que entreguen los datos y la información que constituyen a todas luces, las fuentes de prueba del delito, sino que requieren que con carácter previo el juez de instrucción competente autorice dicha entrega, previa solicitud y de conformidad con los presupuestos y requisitos de la concreta diligencia de investigación que proceda en cada caso. De forma análoga, los miembros del Ministerio Fiscal también ven limitada su capacidad de actuación y maniobra en estos supuestos cuando se encuentren al frente de una investigación preliminar por mor de la recepción de una *notitia criminis* por la comisión de un delito de odio y deben de acudir consecuentemente al juez de instrucción para obtener información relativa a las comunicaciones electrónicas o a servicios de la sociedad de la información.

Esta limitación de las facultades indagatorias a la que se enfrentan las fuerzas policiales y el Ministerio Fiscal podría derivar en la frustración, o al menos disminución de la capacidad de obtención de las fuentes de prueba necesarias para el buen fin de la investigación de ciertas conductas delictivas cometidas en la red, pues el dictado y entrega de la preceptiva autorización judicial puede requerir de un lapso de tiempo superior a las veinticuatro horas previstas en el art. 588 bis c) LECrim, con el riesgo que dicha demora conlleva. Adviértase que se requiere de la traslación de la oportuna denuncia al Juzgado de Instrucción junto a la solicitud de adopción de actos de la investigación necesarios conforme a lo establecido en el art. 588 bis c) LECrim y el posterior examen del juez antes de que se proceda al dictado de la resolución habilitante, debiendo asimismo ser notificada posteriormente al prestador de servicios.

Para evitar estas situaciones, es por lo que el ordenamiento procesal ha previsto un instrumento jurídico de aseguramiento de fuentes de prueba que permite evitar la desaparición de datos o información de las bases de datos, de entre otros sujetos, proveedores de servicios de comunicaciones electrónicas o de la sociedad de la información, en tanto en cuanto se obtiene la resolución judicial autorizante de la diligencia de investigación: la denominada en nuestra Ley de Enjuiciamiento Criminal como orden de conservación de datos o en el ámbito convencional como orden rápida de conservación de datos o *quick freeze data*. Herramienta que como se va a comprobar a continuación, se convierte en una aliada imprescindible de las autoridades policiales y del Ministerio Fiscal para garantizar la disponibilidad e integridad de la información almacenada en sistemas y archivos informáticos de terceros, que resulte necesaria para la persecución e investigación de los delitos de odio que se cometen a través de la red o mediante la utilización de medios electrónicos.

Regulación de la orden de conservación de datos

Enmarcado en el Capítulo X del Título VIII del Libro II de la Ley de Enjuiciamiento Criminal se localiza el art. 588 *octies*, precepto introducido por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento

Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica[14] con la finalidad de instaurar un nuevo instrumento procesal para el aseguramiento de fuentes de prueba de naturaleza electrónica y al que se ha denominado orden de conservación de datos. Esta novísima herramienta jurídica de gran utilidad práctica y que contribuye notablemente a mejorar la eficacia de las investigaciones relacionadas con los ciberdelitos, halla su origen y configuración en la llamada diligencia de conservación rápida de datos informáticos almacenados prevista en los arts. 16 y 17 del Convenio del Consejo de Europa sobre Ciberdelincuencia de 23 de noviembre de 2001[15]. Instrumento está destinado a asegurar que las autoridades competentes de los Estados parte puedan conseguir de forma ágil y rauda la conservación de datos electrónicos almacenados en un sistema informático[16], especialmente, cuando éstos resulten particularmente susceptibles de una inminente pérdida o modificación[17]. Así pues, con la incorporación a la LECrim de la diligencia de conservación de datos a través del art. 588 *octies*, el legislador nacional dio efectivo cumplimiento a los compromisos asumidos en los referidos preceptos del Convenio de Budapest.

En virtud de esta medida de aseguramiento de fuentes de pruebas, tanto el Ministerio Fiscal como la Policía Judicial se encuentran legitimados[18] para requerir y ordenar, de forma autónoma y sin necesidad de previa orden judicial[19], a un sujeto a que conserve incólume y proteja un dato, un conjunto de

14 «BOE» núm. 239, de 6 de octubre de 2015. BOE-A-2015-10725.

15 También conocido como Convenio de Budapest sobre Ciberdelincuencia, por ser la ciudad en la que tuvo lugar su firma. Fue ratificado por España el anterior 20 de mayo de 2010 y cuyo Instrumento de Ratificación fue publicado en el «BOE» núm. 226, de 17 de septiembre de 2010. BOE-A-2010-14221.

16 OTAMENDI ZOZAYA, F., *Las últimas reformas de la ley de enjuiciamiento criminal: una visión práctica tras un año de vigencia*, Dykinson, Madrid, 2017, p. 147.

17 ASENSIO GALLEGO, J. M., "Los delitos informáticos y las medidas de investigación y obtención de pruebas en el convenio de Budapest sobre la ciberdelincuencia", *Justicia penal y nuevas formas de delincuencia*, dir. J. M. Asensio Mellado, Tirant lo Blanch, Valencia, 2017, p. 56.

18 Nada obsta, a que también el Juez de Instrucción pueda dictar una orden de conservación de datos, por ejemplo, cuando se encuentre a expensas del resultado de otras medidas de investigación acordadas, evitando de este modo la adoptación de medidas limitativas de derechos fundamentales y garantizando la disponibilidad de los datos que potencialmente pueden ser útiles para el esclarecimiento del delito.

19 Sostiene la Fiscalía General del Estado, en la Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal, que por no exigir su dictado orden judicial, la orden de conservación de datos no requiere una motivación especial para garantizar su validez, sin perjuicio de la necesariedad de justificar sucintamente la necesidad de acordar la conservación para posibilitar la eficacia de una ulterior medida que se solicite. De este modo, su validez estaría condicionada a que indicara además, los datos que deben ser conservados, el plazo de conservación y el destinatario de la orden, así como las prevenciones oportunas que permitan la posterior exigencia de responsabilidad penal por delito de desobediencia en caso de no ser atendida la solicitud o no ser respetado el deber de sigilo y reserva que el precepto establece. En este punto, discrepamos de tal parecer y consideramos imprescindible como parte de su

éstos o cierta información concreta y delimitada que se albergue en un sistema informático o de almacenamiento electrónico que se halle bajo su disposición y control, y ello con el objeto de evitar su eliminación o alteración voluntaria o automatizada en tanto en cuanto se obtiene la autorización judicial necesaria que disponga y ordene su ulterior entrega de conformidad con la específica regulación de la diligencia de investigación que se requiera de las previstas en la Ley de Enjuiciamiento Criminal o en cualquier otro instrumento normativo, incluso de cooperación judicial[20]. Y es que se trata de una diligencia de aseguramiento trascendental no solamente en el marco de la investigación de la ciberdelincuencia nacional, sino destinada a jugar un papel fundamental en el ámbito de la cooperación judicial internacional, que es el entorno inspirador del Convenio de Budapest. Por ello la Convención de Budapest prevé en sus arts. 29 y 30 que un Estado parte pueda solicitar a otro que ordene la conservación rápida de datos almacenados por medio de un sistema informático que se encuentre en el territorio de ese otro Estado, respecto de los cuales el Estado requirente tenga la intención de presentar una solicitud de asistencia mutua con vistas al registro o acceso de forma similar, confiscación, obtención o revelación de datos. Es, por tanto, una medida que permite garantizar la inmovilización de ciertos datos que pretenden ser incorporados al proceso como medio de prueba o para su análisis forense, en tanto en cuanto se logre concluir la diligencia judicial requerida para su entrega, sin que se vea frustrada por la eventual desaparición, alteración o deterioro de los datos[21].

La orden de conservación puede tener por objeto la conservación de cualquier modalidad de dato o de información que se halle previamente almacenado en un sistema informático o de almacenamiento[22], pudiendo incluso extenderse a los

contenido, la motivación, siquiera mínima, relativa a la justificación, necesidad y proporcionalidad de la medida, atendiendo las circunstancias del caso, los indicios existentes, los principios rectores de las medidas de investigación y especialmente a la posible contribución de los datos bloqueados a la investigación.

20 ASENSIO GALLEGO, J. M., «Los delitos informáticos y las medidas de investigación y obtención de pruebas en el convenio de Budapest sobre la ciberdelincuencia»…, *op. cit.*, p. 57.

21 El art. 16.1 del Convenio sobre Ciberdelincuencia justifica la razón de ser de esta medida en aquellos supuestos en los que existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación. Lo que justifica QUEVEDO GONZÁLEZ en la vulnerabilidad de las evidencias electrónicas y la posibilidad de que sean destruidas o modificadas bien sea de forma intencional o por procesos automáticos predeterminados. De este modo su posterior aportación como medio de prueba o, en su caso, su análisis forense no se verá frustrado por la desaparición, alteración o deterioro de unos elementos inherentemente volátiles. QUEVEDO GONZÁLEZ, J., *Investigación y prueba del ciberdelito* (tesis doctoral), Universidad de Barcelona, 2017, p. 192. Disponible en https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y. (Fecha de consulta 16 de enero de 2023).

22 Nótese que el art. 588 octies LECrim se refiere de manera genérica a "datos o informaciones concretas", sin establecer ningún tipo de límite en cuanto a la naturaleza de los datos objeto de conservación. La Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal, también mantiene un criterio amplio y señala como posibles datos objetivo de la orden a: "El contenido de

datos alojados en servidores externos o en sistemas *cloud* o virtuales[23]. Además, no debe haber inconveniente legal en que la orden de conservación no se refiera exclusivamente a datos previamente conservados, sino que también conmine a la conservación de datos adicionales cuya generación o captación sea posterior a su emisión, ya de forma inminente o previsible durante el plazo por el que se extienda la medida, evitando con ello la reiteración de sucesivas órdenes en el tiempo conforme se va generando información susceptible de aprehensión[24].

La orden de conservación puede instarse en el desarrollo de la instrucción de cualquier delito tipificado en el Código Penal para la que pueda requerirse acceso a datos electrónicos, sin que exista ningún tipo de limitación legal que atienda a la modalidad delictual o a su gravedad. No obstante, debe tenerse en cuenta que la posterior diligencia de investigación que se tramite para que se acuerde la entrega efectiva de los datos al órgano judicial para su incorporación a los autos, si se sujetará a los presupuestos y demás exigencias que le sean propios. Por tanto, es la posterior entrega de los datos, la que se encontrará supeditada al cumplimiento de los requisitos exigidos en la legislación procesal para la práctica de la medida de investigación que se utilice para conseguir su cesión de los sistemas informáticos del proveedor a las autoridades penales competentes.

comunicaciones telefónicas y telemáticas (art. 588 ter b). Los datos electrónicos de tráfico o asociados a procesos de comunicación, así como los que se produzcan con independencia del establecimiento o no de una concreta comunicación (art. 588 ter b). Los datos electrónicos, diferentes de los anteriores, conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole (arts. 588 ter j, k, l y m). Los datos contenidos en ordenadores, instrumentos de comunicación telefónica o telemática, dispositivos de almacenamiento masivo de información digital o repositorios telemáticos de datos (arts. 588 sexies a, a 588 septies a). Se comprenden, en consecuencia, tanto los datos de tráfico y accesorios cuyo deber de conservación entre ya dentro de las obligaciones que el art. 3 de la Ley 25/2007, de 28 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones impone a los operadores de comunicaciones electrónicas, como cualesquiera otros que pudieran encontrarse almacenados en un sistema accesible o no por el investigado (entre los primeros, su correo electrónico o su cuenta de almacenamiento en la nube; entre los segundos, los datos almacenados en redes sociales, por ejemplo)". No obstante, en este sentido, discrepamos de la posibilidad de que dicho instrumento sea utilizado para conservar preventivamente el contenido material de las comunicaciones que se mantengan por vía telefónica, habida cuenta de que las mismas no son objeto de registro y almacenamiento simultáneo en un archivo o base de datos.

23 RAYÓN BALLESTEROS, M. C., "Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015", *Anuario jurídico y económico escurialense*, núm. 52, 2019, p. 203.

24 En cambio, el criterio de la Fiscalía General del Estado plasmado en la Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal, parece que. La medida se va a referir, siempre, a datos que ya existen y están almacenados, parece rechazar que puedan ser objeto de una orden de conservación los datos pendientes de generación, al indicar que "La medida se va a referir, siempre, a datos que ya existen y están almacenados".

La orden de conservación puede dirigirse no solo a los operadores de comunicaciones electrónicas para la custodia de los datos de tráfico, sino a los proveedores de servicios de internet y, en general, a cualquier persona física[25] y jurídica que tenga a su disposición o bajo su control sistemas informáticos u electrónicos en los que se almacene cualquier tipo de información que pueda ser relevante para la investigación o enjuiciamiento de delitos[26]. En todo caso, en los supuestos en los que los sistemas no se encontraran bajo el dominio o disposición del sujeto al que se dirija la orden, la autoridad deberá de dirigirse al prestador de servicios titular del sistema de almacenamiento, a fin de asegurar un correcto cumplimiento de la medida conservativa.

En consecuencia, se trata de una medida de aseguramiento que cobra sentido en aquellos supuestos en los que no se dispone de forma inminente de la respectiva autorización judicial para el acceso a aquellos, pese a ser requerida, permitiendo asegurar que el titular o responsable de los mismos no proceda a su cancelación, destrucción o alteración. Por ello, el responsable o titular del fichero o sistema informático requerido por la Policía Judicial o Ministerio Fiscal vendrá obligado a prestar su plena colaboración en la ejecución de la medida, debiendo conservar y proteger los datos a los que se circunscriba la orden en el mismo sistema informático en que se hallen y en idéntico estado y situación a la que se encontraran en el momento de recibir la misma, hasta la recepción de la oportuna orden judicial o alternativamente hasta la expiración del plazo recogido en la orden. Es decir, el destinatario de la orden será responsable de mantener la integridad e indemnidad de la información objeto de entrega, garantizando su inmutabilidad respecto al momento al que se refiera la orden. Y para la consecución de ello deberá de un lado adoptar todas las medidas técnicas y organizativas que se requieran para lograr la conservación de la información en las condiciones expresadas – por ejemplo, efectuando copias de seguridad de la información en sistemas paralelos- y de otro lado, impedir que el titular de los datos o el propio sistema informático lógico que gestione las bases de datos alteren voluntaria o automáticamente la información objeto de entrega.

Igualmente, el sujeto obligado al cumplimiento de la orden deberá consecuentemente que rechazar de plano las solicitudes de ejercicio de los derechos de supresión, oposición o rectificación vinculados al derecho a la protección de datos de carácter personal que pudiera instar el interesado al que pertenezca la información. Por ello, habida cuenta del objeto de la orden de conservación,

25 En este punto la Fiscalía General del Estado mantiene que no estarán exceptuados de su cumplimiento ni los parientes del investigado ni quienes resulten amparados por el secreto profesional (como podría ser su abogado). Y ello debido al silencio que guarda la Ley sobre este punto, a diferencia de los casos en los que el legislador ha exceptuado a estas personas (arts. 588 sexies c.5 y 588 septies b.2 LECrim) y al hecho de que el cumplimiento de la orden supone un comportamiento neutro que no puede equipararse a la prestación de una declaración o a cualquier otra colaboración activa en la persecución del delito.

26 TEJADA DE LA FUENTE, E., "La retención obligatoria de datos de tráfico de las comunicaciones electrónicas y telemáticas y la preservación específica de datos informáticos como herramientas de investigación criminal", *El Derecho de Internet*, coord. F. PÉREZ BES, Atelier, Barcelona, 2016, p. 342.

podría decirse que es medida análoga en cuanto a sus efectos a la del bloqueo o limitación de datos prevista en la normativa del derecho protección de datos de carácter personal, que si bien, amén de ser instada por una autoridad facultada en lugar del interesado, extiende su alcance material a cualquier tipo de información que pueda conservarse en un sistema informático y no exclusivamente a datos de carácter personal. En cualquier caso, ello no impedirá que una vez entregados los datos a las autoridades o caducada la orden de conservación de datos sin que se hubiera recibido la autorización judicial oportuna, pueda atender el derecho de supresión que se hubiera solicitado, siempre y cuando concurran los requisitos exigidos en la normativa específica que resulte de aplicación.

Una vez notificada a su destinatario una orden de conservación de datos, éste deberá de conservar en su integridad los datos concretados por el plazo que el órgano requirente hubiera fijado en la misma, el cual deberá atender al previsible plazo que se considera necesario para la tramitación del instrumento judicial por el que se pretenda obtener la cesión de los datos, sin que en ningún caso pueda sobrepasarse inicialmente el plazo de noventa días[27]. No obstante, la regulación nacional prevé la posibilidad de que las autoridades competentes acuerden una eventual y única prórroga del periodo de conservación inicial cuando el plazo fijado no hubiera resultado suficiente para la obtención de la orden judicial o cuando su solicitud se retrasare a expensas de la obtención de avances de la investigación. En tal supuesto, la medida se podrá extender por el plazo necesario para completar la obtención definitiva de la autorización judicial, sin que en ningún caso pueda superarse el plazo de ciento ochenta días desde la emisión de la orden inicial[28].

Una vez expirado el plazo fijado como límite, bien en la orden inicial o bien en la prórroga, sin que se hubiera recibido la concreta orden judicial de entrega o acceso, el responsable del sistema informático no vendrá obligado a prolongar la conservación de los datos requeridos, sin perjuicio de que por otra norma legal pudiera venir impuesta su custodia por un periodo mayor. Mientras que para el caso de que vigente la orden de conservación se obtuviera la autorización judicial correspondiente a la diligencia de investigación por la que se concediera acceso a los datos conservados, el responsable o titular de la base de datos estaría obligado a entregar éstos al agente facultado o autoridad competente que se hubiera determinado en la resolución habilitante y bajo las condiciones fijadas.

En último lugar hay que hacer mención al deber de secreto que adquiere el destinatario de la orden sobre la propia diligencia y que se extiende durante no únicamente durante el periodo en que se extienda su desarrollo, sino incluso con posterioridad con carácter indefinido, so pena de incurrir en la responsabilidad penal reseñada en el apartado 3º del art. 588 *ter e*) LECrim prevista para el

27 Plazo máximo que el legislador nacional ha establecido de conformidad con lo previsto en el art. 16.2 del Convenio de Budapest, en el que se fija la duración de la medida en un máximo de noventa días.

28 Nuevamente, a la hora de establecer el plazo máximo de duración de la medida, incluida la prórroga, se establece el

supuesto de la interceptación de las comunicaciones telefónicas y telemáticas, esto es, en un delito de desobediencia grave[29].

Conclusiones

Por lo expuesto en el presente trabajo, no cabe duda de que la orden de conservación de datos es una novedosa herramienta procesal de aseguramiento de datos a disposición de la Policía Judicial y del Ministerio Fiscal que se convierte en esencial para la investigación no únicamente de los delitos de odio cometidos por vía electrónica, a través de algún medio o servicio de comunicaciones electrónicas o de la sociedad de la información, sino de cualquier otro delito consumado por esta vía.

Su utilización permite garantizar la disponibilidad e integridad de las fuentes de prueba del delito de naturaleza electrónica, minimizando los riesgos de desaparición o alteración que pueden tener origen en el propio victimario o en factores ajenos a éste.

En todo caso, la plena efectividad de la orden de conservación requiere de una actuación rápida y proactiva de la autoridad competente, puesto que deberá anticipar con la mayor antelación posible sobre qué información electrónica es necesario actuar e identificar al prestador o proveedor titular de los servidores o servicios en los que se aloja aquella, dado que cuando más tiempo transcurra entre la comisión del delito y la inmovilización de los datos, más probabilidad existe de que se eliminen o alteren los contenidos delictivos o los rastros y vestigios electrónicos o digitales de la acción ilícita.

Referencia

Delgado Martín, J. (2013). «La prueba electrónica en el proceso penal» en *Diario La Ley*, núm. 8167.

González Jiménez, A. (coord.) (s.f.). «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes» en *Revista de Internet, Derecho y Política*, núm. 27, pp. 17-29.

Asensio Gallego, J. M. (2017). «Los delitos informáticos y las medidas de investigación y obtención de pruebas en el convenio de Budapest sobre la ciberdelincuencia» en Asensio Mellado, J. M. (dir.), *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Valencia, pp. 44-67.

29 Advierte OTAMENDI ZOZAYA acerca del silencio que guarda la LECrim sobre las consecuencias legales que depararía al sujeto obligado el incumplimiento del sujeto obligado del deber de colaboración y cumplimiento de la orden de conservación de datos, lo que no sucede respecto a otras diligencias de investigación contempladas en la misma norma. Sin embargo, considera el autor que cuando éste incumpliere la misma de forma voluntaria e intencionado incurrirá en un delito de desobediencia grave a la autoridad tipificado art. 556 Código Penal. *Vid*. OTAMENDI ZOZAYA, F., *Las últimas reformas de la ley de enjuiciamiento criminal: una visión práctica tras un año de vigencia*, Dykinson, Madrid, 2017, p. 148.

Otamendi Zozaya, F. (2017). *Las últimas reformas de la ley de enjuiciamiento criminal: una visión práctica tras un año de vigencia*, Dykinson, Madrid.

Quevedo González, J. (2017). *Investigación y prueba del ciberdelito* (tesis doctoral), Universidad de Barcelona.

Rayón Ballesteros, M. C. (2015). «Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015» en *Anuario jurídico y económico escurialense*, núm. 52, 2019.

Tamarit Sumalla, J. M. (2018). «Los delitos de odio en las redes sociales» en *Revista de Internet, Derecho y Política*, núm. 27, 2018, pp. 17-29.

Tejada de la Fuente, E. (2016). «La retención obligatoria de datos de tráfico de las comunicaciones electrónicas y telemáticas y la preservación específica de datos informáticos como herramientas de investigación criminal» en Pérez Bes, F. (coord.) *El Derecho de Internet*, Atelier, Barcelona, 2016, p. 315-345.