ACCESO PROCESAL A DATOS ALOJADOS EN EL PROVEEDOR DE SERVICIOS DE TELECOMUNICACIONES (TSP) SEGÚN LA ORDENANZA PROCESAL PENAL ALEMANA (REF. ESP. §100G STPO)

Procedural access to data hosted into the telecommunication server provider (TSP) according to the German procedural criminal Law. (Ref. §100g StPO)

Darío Nicolás Rolón[*]

Resumen: Este artículo se centra en el caso del acceso procesal a datos/información que es objeto de transferencia o que ha sido transferida y se encuentra almacenada en el servidor del proveedor de servicios de telecomunicaciones según la ley procesal penal alemana (ref. §100g StPO). El acceso a datos/información presupone determinar cuál es la garantía constitucional aplicable (secreto de las comunicaciones [Art. 10, GG], protección contra los secuestros y allanamientos irrazonables [Art 13 GG], derecho a la auto-determinación informativa [Art. 10.2 GG], etc.) aplicables a los siguientes tres casos objeto de este artículo: a) casos de acceso a datos/información que actualmente se encuentra siendo transferida por correo electrónico [§100a-b and 103 SPO], b) casos de acceso a datos/información que actualmente se encuentra siendo transferida aunque sin empleo del correo electrónico [§§94-97, StPO], c) casos de acceso a información que ya ha sido transferida y que se encuentra alojada en el servidor de telecomunicaciones [§100g StPO]. Para delinear el campo teórico de las garantías constitucionales mencionadas anteriormente se propondrá examinar la relación entre dos sistemas conceptuales: el primero, formado por conceptos prescriptos en la ley alemana y comunitaria europea, tales como comunicación, información y diferentes tipos de datos (datos de tráfico, datos de posicionamiento global, datos personales, etc.), y el segundo formado por conceptos tradicionales procedentes de la teoría general de la ley penal y procesal penal (tales como delito con significado relevante, delito cometido con el empleo de medios de telecomunicación, [§100g StPO], etc.). Esa relación conceptual será estudiada interrogando sobre si existe una hipótesis puente entre los sistemas mencionados anteriormente.

Palabras clave: Ley de telecomunicaciones – acceso a datos/información – secreto de las comunicaciones – protección contra allanamientos y secuestros ilegales – derecho a la autodeterminación informativa – servidor de telecomunicaciones – correo electrónico –

[*] LLM, Goethe Universität, Frankfurt am Main. La versión en alemán de este texto fue presentada con motivo del seminario organizado los profesores Dr. Christoph Krehl und Dr. Lutz Eidam denominado "Neue Ermittlungsmaßnahmen", correspondiente al semestre de invierno 2014/2015 de la Facultad de Derecho de la Goethe Universität Frankfurt a. M. A la versión original se le hicieron algunas incorporaciones adicionales, como la traducción total o parcial de algunas citas legales, para su mejor comprensión en el idioma castellano, y fue actualizado de conformidad con la ley de reformas del 15 de octubre de 2015.

Este artículo fue recibido el 6 de noviembre de 2015, siendo aprobada su publicación el 28 de diciembre de 2015.

datos de tráfico – datos de posicionamiento global – hipótesis puente.

Abstract: This article focuses on the case of getting procedural access to data/information which is currently transferred or has been already transferred, and hosted by telecommunication-server providers according to German criminal procedural legislation (ref.§100g StPO). Getting procedural access to this data/information presupposes determining the constitutional safeguard (secrecy of communication [Art. 10, GG], protection against unreasonable searches and seizures [Art 13 GG], right to informative self-determination [Art. 10.2 GG] etc.) applicable to the following three cases, scope of this article: a) cases of getting access to data/information which is currently being transferred by using e-mail [§100a-b and 103 SPO], b) cases of getting access to data/information which is currently being transferred, but without using e-mail [§§94-97, StPO], c) cases of getting access to data/information which has been already transferred, and has been hosted into the telecommunication-server [§100g StPO]. In order to delineate the theoretical field of the before mentioned constitutional safeguards, it will be proposed to examine the relation between two conceptual systems: the first one formed by concepts enacted in German and European Communitarian Law (and its judicial interpretation in German and in the European Court) such as communication, information and different kind of data (traffic-data, global positioning-data, personal-data, etc.), and the second one formed by traditional concepts proceeding of the general theory of procedural and criminal law (such as Relevant-Crime, Crime by using of telecommunication-media [§100g StPO] etc.). This conceptual relation will be studied by asking if there are some bridge hypothesis between the before mentioned systems.

Keywords: Telecommunication-Law – access to data/information – secrecy of communication – protection against unreasonable search and seizures – right to informative self-determination – telecommunication-server – e-mail – traffic-data – global positioning data – bridge hypothesis.

I. Introducción

La aplicación de la garantía del secreto de las comunicaciones (art. 10 Ley Fundamental Alemana, en adelante, en sus siglas en el idioma de origen "GG") y la garantía que protege el derecho a la autodeterminación informativa (art. 2 párr. 1 en función del art. 1 párr. 1 GG) no depende únicamente de disposiciones normativas a nivel europeo o alemán, sino también de aspectos técnicos complejos de la comunicación y de la transferencia de información y datos.

La modificación de definiciones técnicas, la mayoría de las cuales se encuentran en las directrices europeas, la Ley de Telecomunicaciones Alemana (en adelante mencionada por sus siglas en alemán: "TKG") y la Ley Federal de Protección de Datos (en sus siglas en idioma originario: "BDSG"), repercute sensiblemente en la interpretación de la Ordenanza Procesal Penal Alemana (en lo sucesivo mencionado por sus siglas en alemán: "StPO"), especialmente en lo que respecta a las medidas procesales para acceder al servidor del proveedor de

servicios de telecomunicación de acuerdo con el §100g StPO.[1]

La discusión sobre la reciente modificación de la Ley de Almacenamiento de Datos (Vorratsdatenspeicherungsgesetz)[2] vuelve a tornar actual el debate sobre las posibilidades estatales en el marco de una investigación penal para acceder a datos relacionados con las personas (personenbezogene daten) y a datos personales (o datos sensibles) alojados en bases de datos bajo el control de proveedores de servicios de telecomunicaciones.

No me ocuparé de la problemática en su totalidad (lo que incluiría, por ejemplo, discutir sobre los límites del "receptación de datos" [§202d StGB],[3] entre otros aspectos igualmente densos), sino solo de algunos aspectos parciales del problema.

---

[1] StGB= Código Penal Alemán, §100g [NT: sección que aquí se analiza]: (1) Si determinados hechos fundamentan la sospecha de que alguien es autor o partícipe 1. ha preparado a través de un delito, ha cometido, ha intentado cometer un delito que tiene también en el caso particular una relevancia significativa, especialmente un delito mencionado en el §100a párrafo 2, en casos en los que la tentativa es punible, o, 2. ha cometido un delito a través de un medio de telecomunicación, se deben recolectar datos de tráfico (§96 párrafo 1 de la ley de telecomunicaciones), en la medida en que ello sea necesario para la averiguación de un hecho, y la recolección de los datos se encuentre en una relación proporcionada con la relevancia de la cuestión. En el caso de la oración 1 número 2 sólo está permitida la medida cuando la averiguación del hecho de otro modo no sería posible. La recolección de datos de posicionamiento sólo es posible según ese párrafo para datos de tráfico futuros o en tiempo real, o sólo está permitida en el caso de la oración 1 número 1, en la medida en que sea necesaria para la averiguación del hecho o la averiguación del lugar de residencia del acusado. (2) Si determinados hechos fundamentan la sospecha de que alguien ha cometido como autor o participe un delito especialmente grave mencionado en el párrafo 2, o en los casos en los que la tentativa es punible, ha intentado un delito semejante, y, en el caso concreto, el delito es especialmente grave, pueden ser recolectados los datos de tráfico almacenados según el §113b de la ley de telecomunicaciones, en la medida en que la averiguación del hecho o la averiguación del lugar de residencia del acusado fuera de otro modo esencialmente dificultosa o no carecería de perspectivas, y la recolección de datos esté en una relación proporcionada con la relevancia de la cuestión. (…). (3) La recolección de todos los datos de tráfico en una señal electromagnética (Funzellenabfrage) sólo está permitida: 1. Cuando los presupuestos del párrafo 1 oración 1 número 1 se encuentran cumplidos, 2. En la medida en que la recolección de datos en un contexto adecuado es relevante para la cuestión y, 3. En la medida en que la averiguación del hecho o la averiguación del lugar de residencia del acusado sería de otra manera muy dificultosa o no tuviera chances de éxito. Se debe acceder a los datos de tráfico almacenados según el §113b de la ley de telecomunicaciones para solicitar datos de ondas electromagnéticas solo bajo los presupuestos del párrafo 2 (...)

[2] BT-Drucksache 18/5088, 15 de octubre 2015.

[3] StGB, §202d: Receptación de datos: [NT: traducción de la parte con mayor relevancia a fines ilustrativos] 1. Quien se procura datos (§202a párrafo 2) para si mismo o para otra persona que no son accesibles para el público en general y que han sido obtenido por otro mediante la comisión de un delito, cede a un tercero, distribuye, o de otro modo lo hace accesible, para enriquecerse o para enriquecer a un tercero, o para perjudicar a otro, será reprimido con una pena privativa de la libertad de hasta tres años o con pena de multa. 2. La pena no puede ser más grave que el delito previo amenazado con pena (...).

En primer lugar me ocuparé de la discusión sobre los límites y la extensión del resultado de la interacción entre conceptos teóricos, cuya relevancia para la discusión no será objetada y que proceden de campos teóricos ajenos al derecho procesal penal (a este problema se lo denominará: *problema de la emergencia conceptual).*[4] Esta cuestión se advertirá, por ejemplo, en el examen de las relaciones conceptuales: dato de posicionamiento (GPS)/comunicación, y correo electrónico/esfera de dominio sobre los datos (*infra* II.1.).

En segundo lugar me detendré en el examen del resultado de la interacción entre conceptos teóricos como "correo electrónico" o "comunicación" sobre las disposiciones procesales que autorizan el acceso a la información.[5]

Finalmente, en lo que respecta al problema vinculado al origen de las disposiciones objeto de análisis (principio genético),[6] en particular las directrices de la Unión Europea y su relación con las reformas legales introducidas en la Ordenanza Procesal Penal Alemana, la doctrina dominante alude usualmente a lucha contra el terrorismo, como una de las principales fuentes del debate sobre la entrada en vigencia de las disposiciones procesales incorporadas al StPO cuya interacción aquí se analizará. No me detendré en todas las posibles fuentes de la discusión en torno a la formación o implicaciones del concepto *terrorismo,* ni tampoco en todas las connotaciones que surgen de la relación causal entre el concepto de terrorismo y la entrada en vigencia de todas las disposiciones sustantivas y/o procesales que podrían tener alguna relevancia en la interpretación de las normas y los casos que aquí se presentan, por exceder el objeto de este trabajo; solamente me ocuparé de la relación que se plantea entre el argumento centrado en la lucha contra el terrorismo con los fundamentos de las normas que confieren competencia a la Unión Europea, (art. 95 EGV) para la promulgación de las normas que son objeto de estudio y cuya incidencia en los derechos fundamentales resulta innegable.

II. Datos relacionados con las personas y protección constitucional

Esta sección tiene como finalidad evidenciar el tipo de relación y los problemas que se plantean entre la garantía que protege el secreto de las comunicaciones con el derecho a la autodeterminación informativa. Recurriré a casos de acceso a información que se transfiere vía correo electrónico, para demostrar los contornos difusos y la relación compleja de ambas garantías.

---

[4] BUNGE (2001), p. 82.

[5] Las hipótesis que permiten vincular los diferentes marcos teóricos serán denominadas, siguiendo la nomenclatura moderna, "hipótesis puente" (*bridge hypothesis*) sobre esto ver: BUNGE (2001), p. 173

[6] *Ibid*, p. 26.

1. La garantía que protege el secreto de las comunicaciones (art. 10 GG) y derecho a la autodeterminación informativa (Art. 2 párr. 1 en función del art. 1 párr. 1 GG)

La garantía que protege el secreto de las comunicaciones según el art. 10 (GG) protege el tráfico de noticias, o en otras palabras, el envío y recepción de mensajes[7] y concurre técnicamente parcialmente con el "derecho a la autodeterminación informativa". [8] La garantía que protege el secreto de las comunicaciones comprende los datos de contenido, el proceso de transferencia de datos, así como todos los datos que guardan relación con las "circunstancias próximas a la comunicación".[9]

El derecho fundamental a garantizar la confiabilidad e integridad de los sistemas técnicos informáticos[10] resulta aplicable a hipótesis que involucran datos relacionados con las personas (personenbezogene Daten)[11] que, según el §3 párr. 1 BDSG, son "datos individuales sobre las circunstancias personales o materiales de una persona natural determinada o determinable".

La definición del concepto "datos relacionados con las personas" es tan amplia que comprende a los ya conocidos "datos de contenido" y de "tráfico",[12] así como también a los datos de ubicación o posicionamiento, que son aquellos que se procesan en una red de comunicación electrónica y que suministran información sobre la ubicación geográfica del aparato electrónico de un usuario de un servicio de comunicación electrónico,[13] y que habilitan la técnica denominada *profiling*, que consiste en la formación de un "perfil de riesgo" de una persona de acuerdo con los hábitos que evidencian sus datos de ubicación geográfica (la técnica del *profiling* naturalmente no es compatible con las premisas básicas del derecho penal de acto, pues el criterio de selección de potenciales infractores radica en el examen de sus hábitos).

Dado que los datos de posicionamiento (GPS) son un subconjunto de datos pertenecientes a la categoría "datos relacionados con las personas" (ver §3 párr. 1 BDSG). Una hipótesis que involucre la recolección no autorizada de los datos de posicionamiento habilitaría al afectado a invocar la garantía que protege el secreto de las comunicaciones (art. 10 GG). El BVerfGE, sin embargo, considera que las hipótesis que habilitan la aplicación de la garantía que protege el secreto de las comunicaciones no se integran únicamente por la categoría "datos relacionados

---

[7] WELP (1994), p. 295.
[8] Artículo 2 Párr. 1 en función del artículo 1 párr. 1 GG.
[9] También llamados "datos de tráfico". La definición de datos sobre las circunstancias próximas a la comunicación se encuentra en el §96 TKG y 113b TKG ver: SCHENKE (2000), p. 19.
[10] Del mismo modo está previsto en el artículo 2 párr. 1 en función del art. 1 párr. 1 GG.
[11] También se los puede llamar "datos personales".
[12] KORN (2009), p. 114.
[13] Art. 2, "C", EU-2002/58/EG.

con las personas", sino que además requieren la existencia de "comunicación".[14]

En función de ello, podría construirse la siguiente regla:

R1: La garantía que protege el secreto de las comunicaciones es aplicable cuando, en forma no autorizada, se recolectan datos relacionados con las personas en el transcurso de una comunicación.

Considerando que la existencia de datos de posicionamiento no depende de la existencia de comunicación, la garantía que protege el secreto de las comunicaciones no debería tener aplicación a los casos de recolección de datos de posicionamiento, si no existe comunicación. La garantía aplicable, cuando no existe comunicación, de acuerdo con la jurisprudencia del BVerfGE, es el derecho a la autodeterminación informativa.[15]

El derecho a la autodeterminación informativa es una derivación del derecho informático fundamental[16] y procede de la jurisprudencia del BverfGE en el caso "Volkszählungsurteil" (BVerfGE 65, 1). Este derecho emerge de dos fuentes: por un lado, la garantía de la inviolabilidad del domicilio (art. 13 GG) y; por el otro, la garantía que protege el secreto de las comunicaciones (art. 10 GG).[17] Por medio del derecho a la autodeterminación informativa se pretendió hallar respuesta a varias interrogantes que provenían especialmente del campo de la criminalidad informática, entre ellos, por ejemplo, la pregunta sobre la posibilidad de secuestrar datos transferidos durante el proceso de comunicación.[18]

---

[14] BverfGE, 1 BvR 256/08, 2 de marzo 2010.

[15] BverfGE 2 BvR 2099/04 (Segundo Senado)- Sentencia del 2 marzo de 2006 (LG Karlsruhe); Pagekopf, Martin/, Art. 10 GG in: SACHS (2014), p. 498, Korn (2009), p. 113. No es claro, sin embargo, si se puede invocar la garantía que protege el secreto de las comunicaciones, cuando, durante el transcurso de la comunicación, se recolectan datos de posicionamiento. En tal caso, podría sostenerse que los datos de posicionamiento son datos relacionados con las personas, y, por lo tanto, deberían estar amparados por la garantía que protege el secreto de las comunicaciones. La recolección de datos de posicionamiento, con fundamento en una excepción a la garantía que protege el secreto de las comunicaciones, debería estar circunscripta únicamente al tiempo que dura la comunicación.

[16] O también: *Computer-Grundrecht*, cuya una traducción exacta al idioma castellano no es posible.

[17] SCHENKE (2000), p. 22/3.

[18] Por ejemplo, como sucede con la instalación de dispositivos de vigilancia, en el caso de vigilancia acústica u óptica, que se rige por la garantía que protege la inviolabilidad del domicilio, por estar expresamente previsto como excepción. BverfGE 2 BvR 902/06 (3ra. cámara del Segundo Senado) Sentencia del 29 de junio de 2006, Nr. 17: Pero cuando la medida afecta derechos de terceros, se tiene que aplicar el principio de proporcionalidad. BverfGE 2 BvR 902/06 (3ra. cámara del Segundo Senado) decisión del 29 de junio de 2006, Nr. 18. También: Landgericht Hanau (Az.: 3 Qs 149/99 decisión del 23.09.1999): El sistema de correo electrónico consiste en la transmisión de información con almacenamiento intermedio y, por lo tanto, se encuentra comprendido por la garantía que protege el secreto de las comunicaciones. En consecuencia, entra en consideración el §100a StPO. El LG Hanau decisión del 23.09.1999 (3 Qs 149/99) estableció que los correos

El ámbito de validez de este nuevo derecho se extiende también a las hipótesis que comprenden los datos de posicionamiento geográfico. En ese sentido, algún sector de la doctrina ha sostenido que este derecho guarda una relación de especificidad con respecto a la garantía que protege el secreto de las comunicaciones; sin embargo, para el BVerfGE ambas garantías se superponen parcialmente.[19]

Una posible razón que explica la superposición de las garantías y la dificultad para delimitar sus ámbitos de validez radica en los límites difusos del concepto de comunicación y de los elementos conceptuales que presupone la comunicación, como por ejemplo, el concepto de transferencia de información y datos, así como también la falta de examen de la influencia de teorías que proceden de otros campos teóricos como, por ejemplo, el concepto "esfera de dominio" o también "dominio" que, en la jurisprudencia del BverfGE a partir del 2006, parece referirse al concepto de "dominio del hecho", empleado habitualmente en el campo de la teoría de la autoría y del concurso de personas. Algunos ejemplos provenientes de la jurisprudencia sobre transferencia de datos e información por correo electrónico permitirían verificar esta *bridge hipothesis*. Veamos.

2. Concurso de garantías: Acceso a los correos electrónicos

La jurisprudencia del BVerfGE y del BGH sobre transferencia de información y datos por correo electrónico plantea, a grandes rasgos, dos clases de problemas: por un lado, el problema sobre los presupuestos y los límites temporales del concepto de comunicación y, por el otro, el problema sobre la aplicación del concepto teórico de "dominio" al campo de la transferencia de información y datos.

Tanto el BVerfGE como el BGH han resuelto que sobre transferencia de información y datos por correo electrónico resultan al menos dos criterios dudosos desde el punto de vista técnico: 1) la aplicación de la garantía que protege el secreto de las comunicaciones a los correos electrónicos cuando la información alojada en el servidor se encuentra exclusivamente en la esfera de dominio del receptor; y 2) la aplicación del derecho a la autodeterminación informativa a los correos electrónicos, cuando se encuentran exclusivamente en el ámbito de dominio del receptor. De estos criterios me ocuparé a continuación.

Según el BverfGE, el presupuesto para la vigencia de la garantía que protege el secreto de las comunicaciones es la existencia de una comunicación a través de un servicio de telecomunicaciones. Con base en esa proposición, el Segundo Senado del BGH ha sostenido la tesis de que una escucha telefónica se

---

electrónicos enviados y almacenados que se encuentran en el servidor de correo, no pueden ser secuestrados con fundamento en los §§94 y ss. StPO. Allí tienen aplicación el §100a StPO.

19 SCHENKE (2000), p. 24. Para examinar la compatibilidad de la ley con la Ley Fundamental el BverfGE exige determinar cuáles han sido los fines del legislador al promulgar las leyes, ver: BverfGE, 120, 274: "*Online-Durchsuchung*"; KUTSCHA/THOMÉ (2013), p. 15.

puede extender también a las manifestaciones realizadas por la persona vigilada que creyó erróneamente que la comunicación había concluido: En la sentencia BGH 2 StR 341/02, el acusado, por error, creyó que el interlocutor ya había apagado el teléfono y continuó hablando sin apagar el suyo, por lo que la policía siguió escuchando sus dichos formulados en voz alta. El acusado argumentó, durante el desarrollo del proceso en su contra, que la escucha telefónica ordenada se limitaba al caso de que existiera comunicación y, que una vez concluida dicha comunicación (tal como lo había supuesto el acusado), la escucha era ilegal. El Segundo Senado del BGH sostuvo que de las circunstancias no surgía claramente para los agentes de policía que la comunicación había concluido, por lo que se mantenía la vigencia de la orden judicial para interceptar la comunicación, aun cuando posteriormente se pudiera comprobar que había razones para pensar que la comunicación había concluido.[20]

A partir de 2006, el BverfGE considera que los §§ 94 y 97 StPO son suficientes para fundamentar el secuestro de la información de los correos electrónicos que se encuentran situados en el servidor del proveedor de servicios de telecomunicaciones.[21] No resulta aplicable la garantía que protege el secreto de las comunicaciones a la información transferida, por estar concluido el proceso de comunicación. Tampoco se encuentra afectado del derecho a la autodeterminación informativa, si la persona investigada no adoptó las medidas necesarias para evitar el acceso a la información ubicada en su esfera de dominio.[22]

El criterio actual del BVerfGE no es nuevo y difiere parcialmente de las

---

[20] BGH 2 StR 341/02-Urteil vom 14. März 2003 (LG Köln), (Nr. 15). Las circunstancias según las cuales la policía no debería haber seguido escuchando no estaban en el caso del todo claras. El BGH convalidó la continuación de la medida (Nr. 16).

[21] §94 StPO:

(1) Los objetos que pueden ser medios de prueba relevantes para la investigación deben ser tomados en custodia o deben asegurados de otra forma.

(2) Si los objetos se encuentran al cuidado de una persona y no son revelados voluntariamente, es necesario ordenar el secuestro.

(3) Los párrafos 1 y 2 rigen también para licencias de conducir.

Por su parte el §97 StPO, en su parte relevante para esta cuestión, prescribe: No corresponde el secuestro:

(1) de las comunicaciones escritas entre los acusados y las personas que tienen permitido negarse a declarar según los §52 o §53 Párr. 1, oración 1 Nr. 1 hasta 3b;

(2) de las grabaciones por medio de las cuales las personas mencionadas en los §53 Párr. 1 oración 1 hasta 3b sobre las que se extiende el derecho a negarse a declarar, hicieron manifestaciones sobre los acusados, u otras circunstancias;

(3) otros objetos que se relacionan con el trabajo médico, sobre el que se extiende el derecho a negarse a declarar previsto en el §53 Párr. 1, oración 1 hasta 3b.

[22] Según el BverfGE 2 BvR 902/06 (3ra. cámara del Segundo Senado) en su decisión del 29 de junio de 2006 (LG Braunschweig/AG Braunschweig) se deben aplicar los §§95, 98 StPO para el secuestro de datos, que se encuentran situados en el servidor. El secreto de las comunicaciones no se aplica a tales datos. (Segundo Senado del BGH, 2 de marzo de 2006, 2 BvR 2099/04).

sentencias anteriores del BGH que equiparaban expresamente la transmisión de datos electrónicos con el correo postal. De acuerdo con el BVerfGE, los §§100 a-b y 103 StPO, que regulan estrictamente la garantía que protege el secreto de las comunicaciones, no tienen aplicación cuando la información a obtener se encuentra situada en el servidor de la empresa de servicios de telecomunicaciones. Las normas aplicables a esa hipótesis son, pues, los §§ 94, 97 StPO, que, por definición, son genéricas respecto de las normas que regulan el secreto de las comunicaciones.[23] El fundamento de ello surge de la regla provisional que se formula, a modo de síntesis, a continuación (R2):

R2: Se puede autorizar el acceso a la información transmitida por correo electrónico que se encuentra alojado en el servidor de la empresa de telecomunicaciones con fundamento en los §§94, 97 StPO siempre que no exista comunicación, o bien su inexistencia haya sido asumida erróneamente por la persona vigilada, se trate de la recolección de datos de posicionamiento, o bien, en caso de que la persona vigilada no haya tomado los recaudos suficientes para excluir del acceso a su información, cuando se encuentra en su esfera de dominio.[24]

La regla (R2) presupone que la información o los datos son equiparables a una cosa material y, por lo tanto, pueden ser secuestrados, y prescribe además que la persona afectada debe adoptar medidas conducentes a evitar el acceso a esa información o datos, cuando la información o los datos se encuentran en su esfera de dominio, de manera que la aplicación de una garantía que protege el secreto de las comunicaciones no depende solamente del concepto de comunicación, sino también de las medidas adoptadas por el titular de los derechos para excluir o impedir el acceso por parte de terceros. La regla no suministra una definición clara, sin embargo, sobre qué se entiende por "esfera de dominio". Tampoco está claro en qué medida guarda analogía los conceptos de "cosa" con de "información" y "dato", ni hasta qué punto se puede equiparar el correo electrónico con el correo

[23] Por ejemplo, BGH 1 Bgs 626/95, 2 Bjs 94/94-6-1BGs 625/95-, decisión del 31 de julio de 1995. El acceso a los correos electrónicos se rige por la garantía que protege el secreto de las comunicaciones. Los §§ 94, 97 StPO no tienen aplicación a los datos electrónicos, a pesar de su similitud con las cosas materiales. Ejemplo: la jurisprudencia anterior a la sentencia BverfGE 2 BvR 902/06 encontraba su fundamento en la Ley de Estructura de Correos del 1 de junio de 1989, y en la sentencia BverfGE de 1997, según la cual la garantía que protege el secreto de las comunicaciones y, por ende, tanto el §100a StPO, como el §103 StPO, también tienen aplicación para los nuevos procesos o sistemas de comunicación BverfGE 2 BvR 902/06 (3ra. cámara del Segundo Senado) decisión del 29 de junio de 2006, Nr. 12 y 13. El Tribunal Federal de Ravensburg es un ejemplo de la aplicación de la regla vigente hasta la sentencia del BverfGE de 2006. El mencionado tribunal aplicó la garantía que protege el secreto de las comunicaciones (Art. 10 GG) al secuestro de la información contenida en los correos electrónicos cuando ésta se encuentra alojada en el servidor de la empresa prestadora de servicios de telecomunicación. Esto significa que el acceso a esa información debe tener fundamento en los §§100 a-b y 103 StPO, ver: Landgericht Ravensburg: Decisión del 09.12.2002, (Az.: 2 Qs 153/02); BverfGE 46, 120, 142 y ss.

[24] Siempre bajo el presupuesto rector: falta de comunicación. Cfr.: BverfGE 2 BvR 2099/04 (segundo senado)- sentencia del 2 marzo de 2006 (LG Karlsruhe), Nr. 74. Esos factores rigen también para los datos almacenados en la SIM-*Card*; ver: SCHLEGEL (2007), p. 46/7.

tradicional. En lo que respecta a los datos GPS, si bien la nueva ley de reformas al §100g StPO dispone, en su artículo 6, que los artículos 1 y 2, referidos esencialmente a la reforma al StPO, afecta a la garantía que protege las comunicaciones, es una simple mención legislativa que pretende regular la garantía, pero que no tiene efecto sobre el grado de concreción de la garantía a hipótesis particulares, tarea propia de la jurisprudencia.

La jurisprudencia pronunciándose sobre correo electrónico presupone la existencia del elemento "comunicación" para la aplicación de la garantía que protege el secreto de las comunicaciones. La pregunta sobre la capacidad de rendimiento del derecho a la autodeterminación informativa en los casos en los que no está presente el requisito de la comunicación debería responderse atendiendo a las posibilidades estatales para requerir información a los proveedores de servicios de comunicación, por ejemplo, al proveedor de servicios de correo electrónico.

A continuación me ocuparé de precisar el estado de la legislación sobre las potestades para recolectar datos, y de las críticas que se le han formulado. De esta manera haré mención a las hipótesis de acceso a datos relacionados con las personas cuando no está presente el requisito de la comunicación, y también al grupo de casos donde el concepto "comunicación" tiene una influencia parcial.

La siguiente sección tiene como finalidad, en primer lugar, responder a la interrogante sobre el origen de las disposiciones que autorizan al acceso a la información que se encuentra almacenada o que es procesada por los servidores de internet; y, en segundo, identificar el grado de concreción de las disposiciones de la Unión Europea en la legislación penal y procesal penal alemana (Ref. esp. § 100g StPO).

III. Acceso a los datos relativos a las personas alojados en la base de datos del proveedor de servicios de telecomunicaciones (TSP) según la Convención sobre Ciberdelincuencia

La Convención sobre Ciberdelincuencia (también llamada "Convención de Budapest") es un convenio de derecho internacional que requiere aprobación, ratificación y posterior introducción en el derecho alemán.[25] La firma de la Convención de Budapest es voluntaria por cada estado miembro.[26] Alemania firmó la Convención sobre Ciberdelincuencia, el 23 de noviembre de 2001. El fin del aludido convenio consiste en la armonización de normas penales sobre criminalidad informática entre los estados parte. Entre las normas que deben ser armonizadas se encuentran aquellas vinculadas con los prestadores de servicios de telecomunicación,

[25] Art. 59, párr. 2 GG, ver: GERCKE (2004), p. 782.
[26] *Ibid.*, p. 783.

previstas en los arts. 16/21. Las normas de mención se aplican a los prestadores de servicios de telecomunicaciones con independencia de que persigan o no, una finalidad comercial.[27] La Convención sobre Ciberdelincuencia no impone, sin embargo, a los proveedores de servicios de telecomunicación deberes tan amplios como lo hace el §100g StPO; solo prevé deberes para casos puntuales.[28]

Tampoco autoriza la vigilancia y recolección discrecional de datos de tráfico.[29] De acuerdo con sus arts. 16 y 17, cada estado miembro debe adoptar las medidas necesarias para garantizar el acceso a los datos de tráfico a los funcionarios a cargo de la persecución penal. En el artículo 16, que se complementa con el artículo 20, se prevé el plazo de nueve días, durante los cuales el prestador de servicios de telecomunicaciones, con independencia que persiga o no un fin comercial, debe tratar en forma confiable los datos,[30] retener e informar sobre los datos de tráfico a solicitud de los funcionarios a cargo de la persecución penal ("*Quick-Freeze*"),[31] en caso de delitos graves.[32]

Desde la entrada en vigencia de la convención se han producido numerosas modificaciones, tanto en el ámbito de la Unión Europea como en la legislación alemana. En lo que concierne a los datos que se relacionan con las personas al nivel de la Unión Europea, se deben tener en consideración dos directrices: La directriz EU-2002/58/EG del 12 de julio de 2002 y la directriz EU-2006/24/EG del 15 de marzo de 2006.

A nivel de la legislación alemana se deben considerar las reiteradas reformas del §100 StPO (especialmente del §100 g StPO). El §100g StPO introducido en 2002, fue modificado en 2007,[33] y entró en vigencia a partir del 1 de enero de 2008;[34] posteriormente el mismo artículo fue nuevamente modificado con motivo de la decisión del BverfGE[35] y entró en vigencia a partir del 10 de marzo de 2010.[36] (Sobre los detalles de evolución legislativa del §100g ver *infra* V I). Finalmente, el 15 de octubre de 2015, el Parlamento Alemán aprobó el proyecto de la coalición de gobierno, e introdujo nuevas modificaciones, especialmente al §100g StPO, entre otros.

---

[27] *Ibid.*, p. 786.
[28] *Ibid.*, p. 787.
[29] *Ibid.*
[30] Art. 20, párr. 3.
[31] Art. 20, párr. 1, A-B.
[32] Art. 20 párr. 4 en relación con el art. 14 párr. 3 A.
[33] Artículo 1 de la "Ley para la Nueva Reglamentación de la Vigilancia de Telecomunicaciones y otras Medidas Encubiertas así como también la puesta en práctica de la directriz 2006/24/EG del 21 de diciembre de 2007".
[34] Boletín Oficial Alemán: BGBl. I p. 3198.
[35] 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 – (con respecto a los §§ 113a y 113b de la ley de telecomunicaciones y el § 100g párrafo 1 oración 1 del StPO de la versión vigente hasta el 2015).
[36] Boletín Oficial Alemán: BGBl. I p. 272.

IV. Acceso a datos relativos a las personas alojados en la base de datos del proveedor de servicios de telecomunicación en el plano de la Unión Europea. El terrorismo y las normas sobre competencia de la UE

1. Almacenamiento de datos y regulación en el plano de la Unión Europea.

a. Directriz EU-2002/58/EG.

El 12 de julio de 2002, el Consejo Europeo promulgó la directriz EU-2002/58/EG sobre el procesamiento de datos. El procesamiento de datos relativos a las personas según la directriz tuvo lugar bajo numerosas condiciones. La disposición en cuestión preveía el borrado inmediato o la adopción de procesos adecuados para el anonimato de los datos por parte de los prestadores de servicios de telecomunicación, luego de concluido el proceso de transferencia de la información. [37] Los prestadores de servicios de telecomunicaciones debían almacenar datos con fines contables dentro de un plazo determinado.[38]

El procesamiento y almacenamiento de datos tenía lugar bajo la condición de que los datos pudieran ser anonimizados, o mediara consentimiento del afectado para su tratamiento.[39] Además, la directriz tenía en consideración los costos económicos en que debían incurrir los prestadores de servicios de telecomunicación para la puesta en práctica de la directriz.[40]

La versión vigente hasta el primero de enero de 2008 del §100g StPO, regulaba la directriz en cuestión en el derecho alemán. El §100g StPO autorizaba a los funcionarios encargados de la persecución penal a requerir información a los prestadores de servicios de telecomunicaciones sobre los datos almacenados en el servidor. La versión vigente hasta el 2008 del §100g StPO preveía el derecho del afectado a solicitar el borrado, supresión o anonimato de los datos, así como también la atribución de consentir y, posteriormente, revocar el consentimiento sobre el procesamiento de los datos.[41] La regla vigente hasta el primero de enero de 2008 sobre el procesamiento y almacenamiento de datos señalaba, pues, que los prestadores de servicios de la comunicación se encontraban obligados, de acuerdo con los requerimientos de la directriz EU-2002/58/EG y §100 g StPO, a dar información a los funcionarios a cargo de la investigación penal.

---

[37] Art. 6.1 EU-2002/58/EG.

[38] El plazo se refiere al período dentro del cual los registros contables pueden ser cuestionados judicialmente, o podría hacerse valer para la pretensión del pago (Art. 6.2 EU-2002/58/EG).

[39] Art. 9, EU-2002/58/EG.

[40] Art. 4.1. EU-2002/58/EG.

[41] Con sustento en los arts. 6 y 9, EU-2002/58/EG.

b. La sentencia de la Corte Europea en el caso 317/8-04 y la lucha contra el terrorismo para la transferencia de información. Límites del art. 95 EGV

En el caso 317/8-04, el procurador general ante la Corte Europea, Philipp Léger, se pronunció a favor de la abrogación de la decisión 2004/4496/CE del Consejo Europeo que autorizaba la transmisión de datos de pasajeros de líneas aéreas a los Estados Unidos de Norteamérica y Canadá,[42] con el argumento de que el artículo 95 EGV[43] solo le atribuye competencias al Consejo Europeo para la transferencia de esos datos, con el fin de la armonización del mercado interno. La Corte europea (en adelante denominada en sus siglas en alemán: "EuGH"), por su parte, en el mismo sentido que el atribuido por el procurador general, sostuvo que la decisión del Consejo Europeo era inválida,[44] y que el artículo 95 EGV no era una razón suficiente para la transferencia de datos a los funcionarios encargados de la persecución penal, porque de dicho artículo no resulta ninguna competencia para el Consejo Europeo a tales fines.[45]

Para el EuGH en los casos C-317/04 y C-318/04 no es suficiente el argumento basado en la armonización del mercado interno para introducir medidas de índole procesal penal, previsto en el artículo mencionado, en el marco de la lucha contra el terrorismo.[46] Si bien el procesamiento de datos cae dentro de las reglas del mercado interno (de hecho, se trata del procesamiento de datos para la venta de billetes aéreos), la decisión del Consejo Europeo de suministrar los datos también tuvo como fundamento la lucha contra el terrorismo, cuestión que excede las competencias previstas en el artículo 95 EGV.[47]

c. Directriz 2006/24/EG del 15 de marzo 2006

La directriz EU-2006/24/EG entró en vigencia el 15 de marzo de 2006, luego de que fracasaran las tentativas del Consejo Europeo para el establecimiento de una tercera columna relativa al almacenamiento de datos dentro de Europa y remplazó a la directriz, por entonces vigente. La directriz vigente a partir de 2006 persigue luchar contra el terrorismo y otros delitos graves y armonizar la legislación vigente sobre el almacenamiento de datos.[48] La puesta en práctica de la directriz no ha sido uniforme en toda Europa.[49]

---

[42] Se los denomina en la sentencia: *Passenger Record Nummer*, "PNR".

[43] Las siglas se refieren al "*Europäischer General Vertrag*" o "Convenio General Europeo". Su versión castellana está disponible, por lo que no es necesaria su traducción.

[44] EuGH, 30.05.2006 - C-317/04, C-318/04, ZÖLLER (2007), p. 408.

[45] ZÖLLER (2007), p. 409; WESTPHAL (2006), p. 712; BREYER (2007), p. 215.

[46] ZÖLLER (2007), p. 409. Ver especialmente el considerando 15 de la decisión, según la cual la lucha contra el terror se encuentra comprendida. Ver: EuGH-Urteil, C.317/8-04, Nr. 55.

[47] EuGH-Sentencia, C.317/8-04, Nr. 55, 58.

[48] Art. 1 párr. 1 EU-2006/24/EG, Considerando Nr. 8-10 RiL 2006/24/EG, artículo 1 párr.1.

[49] De hecho, el EuGH se pronunció en reiteradas oportunidades frente al incumplimiento en la puesta en práctica de la directriz respecto a algunos países de la unión ver: EuGH: Irlanda: C-

La directriz no prevé ni una definición de terrorismo, ni una definición sobre "delitos graves", ni tampoco un catálogo de datos a almacenar. La relación, "dato↔delito grave", debe ser concretizada por cada uno de los estados miembros.[50] En Alemania, por ejemplo, se entiende por "delito grave", siguiendo la terminología del BGH, a los delitos en al ámbito de la criminalidad compleja.[51] Si bien una interpretación amplia de la directiva habilitaría, por ende, la persecución de numerosos delitos que no tienen relación directa con el terrorismo, sin previa adaptación en la legislación y jurisprudencia de cada estado,[52] lo cierto es que también dejar a criterio de cada estado miembro el establecimiento del contenido de la relación "dato↔delito grave" (también "delito con significado relevante"), difícilmente pueda cumplir el objetivo de armonización de la legislación por parte de la directriz.

La directiva impone deberes a los prestadores de servicios de telecomunicaciones o de internet de almacenar datos durante seis meses,[53] aunque no contiene ningún catálogo preciso de cuáles datos a almacenar.[54] La directiva encuentra aplicación a los prestadores de servicios públicos de telecomunicaciones de los estados miembros, con independencia de que los proveedores persigan o no fines comerciales.[55]

d. Examen comparativo: EU-2002/24/EG y EU-2006/24/EG

La directiva EU-2002/24/EG imponía deberes a aquellos que se ocupan de la puesta a disposición pública de servicios de comunicación electrónica en redes públicas de comunicación. La nueva directiva comprende también a aquellos prestadores que incluso no preoporcionan públicamente servicios de comunicación.[56] La directriz EU-2006/24/EG va más allá de la directriz anterior, porque comprende también a los datos internos de las empresas prestadoras de servicios de telecomunicación. La directriz anterior permitía el almacenamiento de

---

202/09, 26.11.2009; Grecia: C-211/09, 26.11.2009; Suecia: C-185/09, 04.02.2010; Austria: C-189/09, 29.07.2010.

[50] WESTPHAL (2006), p. 715/6.

[51] BREYER (2007), p. 217.

[52] Considerando 9/10 RiL-2006/24/EG.

[53] §113a párr. 1, oración 1 TKG en función del §100g StPO; artículo 6 RiL-2006/24/EG, *Westphal, Dietrich, Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten- Brüsseler Stellungnahme zum Verhältnis von Freiheit und Sicherheit in der „Post-911-Informationsgesellschaft"*, EuR, 2006, Nomos, p. 712; Korge, Tobias, *Die Beschlagnahme elektronisch gespeicherter Daten bei privaten Trägern von Berufsgeheimnissen, Springer*, 2009, Berlin, Heidelberg, p. 89.

[54] Art. 5 EU-2006/24/EG. Excluye sin embargo sin embargo excluye a los datos de contenidos, como a los datos del asunto del correo electrónico, y las direcciones (URLs) de los sitios de internet visitados: Art. 6 Párr. 2 RiL 2006/24/EG; BREYER (2007), p. 215.

[55] Art. 1.1. EU-2006/24/EG.

[56] Art. 3.1. EU-2002/24/EG; Korge, p. 89.

datos bajo requerimientos estrictos, y el §100g StPO, vigente hasta 2008, reglamentaba tales requerimientos.[57] La nueva directriz, al igual que el nuevo el §100g StPO, se aparta de los requerimientos previstos anteriormente para el almacenamiento de datos. A ello hay que agregar que, si bien se mantuvo la posibilidad de solicitar el anonimato de los datos, desde 2004 se previó la posibilidad de que los prestadores informaran también sobre los datos de identificación del usuario, lo que dificulta aún más el derecho a solicitar que los datos permanezcan anónimos.[58]

Se ha sostenido que el almacenamiento de datos previsto en la directriz EU-2006/24/EG es incompatible con el artículo 8 párrafo 2 del Convenio Europeo de Derechos Humanos, que requiere una sospecha concreta para acceder a la esfera privada.[59] Si bien según el artículo 5, párrafo 2 RL 2006/24/EG prohíbe almacenar datos que pueden dar información sobre el contenido de la comunicación, con ayuda de los datos "marco" de la comunicación se puede configurar un perfil de las costumbres de comunicación de una persona, lo que legitima el acceso y el registro de información sobre aspectos tanto de la vida como de la comunicación privada por parte de las empresas privadas.[60] No se discute que las empresas ya tuviesen acceso a esos datos, pero, contra la tendencia de reducir el acceso a los datos para preservar la privacidad, la imposición de deberes de registro termina legitimándolo, a la par de restringir las pretensiones dirigidas a suprimir datos, o incluso, a solicitar su anonimato.

Por otra parte, los prestadores de servicios de telecomunicaciones que se encuentran situados fuera de la Unión Europea, se encuentran excluidos del ámbito de vigencia de las directrices europeas. La exclusión de tales empresas del ámbito de la directriz establece, además, condiciones diferenciales para los prestadores de servicios de telecomunicación, lo que podría colisionar con la prohibición de discriminación prevista en el artículo 12 párrafo, GG.[61]

La directriz EU-2006/24/EG, asimismo, reduce la posibilidad de solicitar el anonimato de datos, lo que genera, paradójicamente, el efecto contrario, es decir, la proliferación de técnicas de anonimato y cifrado de datos.[62]

---

[57] EU-2002/24/EG, artículo 6.2. El procesamiento está permitido hasta el fin del plazo, dentro del cual se pueden hacer valer pretensiones para su borrado, o supresión.
[58] §111 TKG Breyer, p. 215.
[59] KLESCZEWSKI (2008), p. 24.
[60] DERKSEN (2011), p. 8.
[61] Art. 19, párr. 3 GG, artículo 18 EUV. Que también rige para personas jurídicas: KUTSCHA/THOMÉ (2013), p. 52. Por otra parte, sin embargo, la imposición de un deber en sí mismo, no siempre implica necesariamente una injerencia a la igualdad laboral, o a la libertad de empresa. Así, no están protegidos, por ejemplo, los intereses comerciales generales o las expectativas comerciales del participante del mercado, en la medida en que su inseguridad sobre la actividad comercial pertenezca a la esencia de los negocios. DERKSEN (2011), p. 11. La afectación viene dada únicamente por la distorsión competitiva que acarrea la directriz.
[62] BREYER (2007), p. 219.

Además, la nueva directriz no tiene en cuenta los costos financieros de implementación en que deben incurrir de los prestadores de servicios de telecomunicación[63] y que acarrean desequilibrios económicos para los prestadores de servicios de telecomunicación dentro de la EU.[64]

Irlanda y Eslovaquia consideraron que la ampliación de las competencias del Consejo Europeo con base en el artículo 95 EGV, así como también el incremento de los costos de implementación para los proveedores dentro de la UE que acarreaba la directriz era ilegal y denunciaron la directiva ante el EuGH.[65]

Sin embargo, frente a tales planteos de los países de mención, el EuGH consideró inicialmente que la directriz era legítima, con el fundamento de que si cada uno de los Estados miembros hubiera implementado disposiciones similares por separado, se habrían producido los mismos efectos en el mercado interno de cada país y de Europa en general. Además, consideró que el artículo 95 EGV era suficiente para el dictado de la directriz, porque preponderantemente regula el funcionamiento del mercado interior.[66]

Bélgica e Irlanda, sin embargo, volvieron a cuestionar la constitucionalidad de la directriz, esta vez con fundamentos en la falta de proporcionalidad de la misma. En esta oportunidad, el EuGH sostuvo en los casos C-293/12 y C-495/12 que la directriz EU-2006/24/EG es incompatible con los arts. 7 y 8 de la Convención Europea de Derechos Humanos. Los fundamentos de la sentencia coinciden *mutatis mutandi* con los argumentos de la BverfGE del 2 de marzo de 2010 (infra V 2).

---

63 A diferencia del artículo 4 EU-2002/58/EG las consecuencias económicas de un deber de almacenamiento son enormes y los costos de implementación luego se transfieren a los usuarios: BREYER (2007), p. 216. DERKSEN (2011), p. 12

64 Los tribunales superiores de Austria y Francia han declarado que es inconstitucional el establecimiento de deberes que conllevan efectos económicos sin prever un deber de indemnización por los gastos en que deben incurrir, ver: BREYER (2007), p. 216. En ese sentido, la versión anterior del §100g StPO no contemplaba costos económicos para las empresas prestadoras de servicios de telecomunicaciones, lo que se traducía en una distorsión competitiva que colisionaba con el artículo 12, GG. El resarcimiento económico ha sido, finalmente, incorporado detalladamente en el artículo 4 de la ley de reformas.

65 El artículo 175 EGV prevé la competencia para los delitos ambientales pero no para la recolección de datos. La competencia de los estados europeos se dirige contra el principio de "empoderamiento limitado" (Art. 249 párr. 1 EGV, arts. 47, 5 EUV), ver: KLESCZEWSKI (2008), p. 22; DERKSEN (2011), p. 19.

66 EuGH C-301/06, 10.02.2009. Nr. 62, 64 y ss.. El caso EuGH C-557/07 del 19.2.2009 es la aplicación del caso C-301/06 a los proveedores de acceso a internet.

V. Acceso a datos relativos a las personas alojados en la base de datos del proveedor de servicios de internet en Alemania

1. §12 Ley de Secreto de las Comunicaciones (FAG) y §§100g, h, StPO

La Ley de Secreto de las Comunicaciones (en su abreviatura en alemán "FAG") fue sancionada en 1928 y modificada en reiteradas oportunidades. Una de las reformas más significativas fue la modificación al §12 FAG de 1989[67] que, debido al incremento y volumen de digitalización de datos, adquirió una importancia hasta antes desconocida. La versión del §12 FAG de 1989 autorizaba al juez a exigir información sobre datos relativos a la comunicación en investigaciones penales, siempre que los datos de la comunicación pudieran conducir a la identificación de los inculpados, o de los hechos a investigar. La potestad se extendía al fiscal, en caso de peligro en la demora.[68]

El §12 FAG fue objeto de varias críticas en el plano constitucional, sobre todo debido a la falta de determinación de los presupuestos de injerencia, además de que la regulación del asunto debía tener lugar en el StPO y no en la FAG. Fue así entonces que el Gobierno Federal presentó un proyecto para la regulación de la cuestión en el §99a StPO.[69] El proyecto incorporaba los requisitos de "realización de un hecho a través de un medio de telecomunicación", "delito con significado relevante". Además, permitía requerir información sobre las "circunstancias próximas a la comunicación", en la medida en que ello fuera necesario para la investigación del hecho, o la averiguación del sitio en el que se encuentra el inculpado.

El artículo 2, párrafo 35 del anexo a la TKG (en sus siglas en alemán "BegleitG") extendió la vigencia de la regla hasta el 31.12.1999, pues no hubo acuerdo para una regla modificatoria que la sucediera. Si bien se mantuvo la vigencia en forma provisoria, se acordó la formulación de un proyecto de §99a StPO, hasta el 30.4.1998, por parte del Gobierno Federal. El proyecto debía, además, asegurar suficientemente el secreto profesional.[70]

Dado que el Gobierno Federal no confeccionó el proyecto, se prolongó la vigencia del §12 FAG hasta el 21.12.2001, al mismo tiempo de que se introdujo el párrafo 2 del §12 FAG, por el cual se declararon aplicables los §100b VI y §100i I oración 1 StPO a los supuestos allí contemplados, lo que

---

[67] GRAFE (2007), p. 23. Por entonces, el requerimiento de informes sobre datos de tráfico no tenía ninguna relevancia, porque los dispositivos de comunicación no permitían almacenar datos luego de concluida la comunicación.

[68] El §12 FAG tenía una vigencia limitada hasta el 31.12.1997 de acuerdo con el §28 FAG, versión 1994, Cfr. GRAFE (2007), p. 24.

[69] Idem, p. 24.

[70] Ibidem.

implicaba, por cierto, el mantenimiento del deber de suprimir la información, una vez examinada.[71]

En 2001, el Parlamento Alemán decidió introducir reglas específicas en el StPO. Aparecieron, entonces, los §§100g y h StPO, con vigencia a partir del 1.1.2002, que modificaron los presupuestos por entonces vigentes en la FAG. A partir de entonces, si bien el fiscal podía solicitar información en caso de peligro de demora, la validez de la medida exigía una validación judicial posterior, dentro de un plazo de tres días.[72] El deber de información se extendía también a los datos de conexión a almacenar en el futuro, además de que se incorporaron los presupuestos: "delito con significado relevante" y "delito cometido por medio de una terminal" en forma definitiva. La vigencia temporal de las nuevas reglas fue fijada hasta el 31.12.2004,[73] luego deberían entrar en vigencia los nuevos literales del §100 StPO, que debían armonizar todas las medidas procesales encubiertas de investigación. El derecho de negarse a declarar en ciertos casos debía ser elaborado en un apartado legal específico.

Al vencimiento del plazo no se cumplieron las metas acordadas, por lo que se prolongó nuevamente la vigencia de los §§100g y 100h StPO, esta vez hasta el 31.12.2007.[74] Finalmente, en ese año, el Parlamento Alemán sancionó la "Ley sobre Nuevas Reglas para la Vigilancia de las Telecomunicaciones y otras Medidas Encubiertas de Investigación así como la puesta en práctica de la Directriz 2006/24/EG", lo que implicó que el requerimiento de datos de tráfico tuviera una ubicación sistemática en el §100g StPO. La ley previó su entrada en vigencia general desde 1.1.2008, y, en el ámbito de internet, desde 1.1.2009.[75]

La versión del §100g StPO de 2007 tuvo vigencia hasta el 15 de octubre de 2015, momento en el que el Parlamento Alemán aprobó el proyecto de la coalición del CDU-CSU y SPD (Unión Democrática Cristiana Alemana, Unión Social Cristiana y Partido Social-Demócrata, respectivamente) que introdujo modificaciones sustanciales tanto al Código Penal (StGB), a la ordenanza procesal penal alemana (StPO) y a la ley de telecomunicaciones (TKG).

2. Sentencia del BverfGE del 2 de marzo de 2010 - 1 BvR 256/08 y, al mismo tiempo, propuesta para la reforma del §100 g StPO

El artículo 1 de la ley de 2007 arriba mencionada introdujo reformas al §100g

[71] Idem, p. 25.
[72] Ibídem.
[73] Ibídem.
[74] En su sesión Nr. 132 del 21.10.2004 el Parlamento Alemán solicitó al Gobierno Federal que, para el 30.06.2007, presente un informe sobre la puesta en práctica de la ley para la prolongación de la vigencia de los §§100g, 100h StPO, desde su introducción. GRAFE (2007), pp. 25/6.
[75] Ídem, p. 26.

StPO, cuya nueva versión entró en vigencia el primero de enero de 2008.[76] La puesta en vigencia de la ley conllevó una serie de planteos de inconstitucionalidad contra los §§113a y b TKG agregados por el artículo 2 número 6 de la ley modificatoria y, también, contra la nueva versión del §100g StPO.[77]

El Primer Senado del BVerfGE consideró que el plazo de seis meses para el almacenamiento de datos previsto en la directriz era incompatible con el artículo 10 GG.[78] El BVerfGE aclaró que el principio de proporcionalidad significaba que el legislador debía prever normas claras y determinadas para asegurar un procesamiento y aseguramiento transparente de datos.[79] Para el BverfGE, el Estado no puede tener acceso directo a los datos que se encuentran alojados en los proveedores,[80] ni le está permitido acumular de datos, sin sospecha previa.[81]

Por otra parte, sostuvo el BVerfGE que el acceso a los datos en el marco de una persecución penal debe suceder según reglas concretas, que deben garantizar la seguridad de los datos,[82] cuya valoración y transmisión debe estar procesalmente asegurada.[83] Los datos a recolectar deben ser diferenciados de acuerdo con su tipo[84] y no pueden ser transferidos o utilizados sin orden judicial previa.[85] El legislador debe prever procedimientos de protección adecuados y sanciones para el caso de abuso de los datos almacenados.[86] Para el BverfGE tales requerimientos no son necesarios, sin embargo, en el caso de información sobre direcciones de protocolo de internet (IP). Lo único que requiere el BverfGE, tratándose de direcciones IP, es una sospecha suficiente o un riesgo concreto sobre una base fáctica puntual.[87]

Por último, el BverfGE declaró que las disposiciones sobre almacenamiento de datos según los §§113a, 113b TKG y §100g StPO eran nulas, y ordenó el borrado de todos los datos hasta entonces almacenados.[88]

---

[76] Boletín oficial alemán: BGBl. I S. 3198.

[77] BverfGE-sentencia del 2 de marzo 2010 - 1 BvR 256/08, Nr. 3.

[78] Ídem, Nr. 205.

[79] Ídem, Nr.. 209.

[80] Ídem, Nr.. 214.

[81] Ídem, Nr. 218.

[82] Ídem, Nr. 221, 228. Las reglas deben el acceso para proteger bienes jurídicos como la vida, la integridad corporal, un peligro común, la existencia del Estado, Cfr. Ídem, Nr. 230.

[83] Ídem, Nr. 235.

[84] Ídem, Nr. 237.

[85] Ídem, Nr. 247.

[86] Ídem, Nr. 252.

[87] Ídem, Nr. 261.

[88] Ídem, Nr. 309. Debe notarse que la nueva versión del §113b TKG prevé nuevos plazos para el almacenamiento de datos: § 113b TKG [NT: se traducirá sólo la parte relevante del §113b TKG a los fines de este trabajo]: Deberes para almacenar los datos de tráfico (1) Los datos mencionados en el §113a párrafo 1 se tienen que almacenar en el interior de la siguiente manera: 1. Los datos según los párrafos 2 y 3 por diez semanas, 2. Los datos de posicionamiento según el párrafo 4 por cuatro semanas; (2) Los prestadores de servicios telefónicos accesibles al público almacenan:1. Los

3. Versión actual del §100g StPO (15/10/2015)

Las modificaciones al §100g StPO en relación con la TKG entraron en vigencia el 10 de marzo, poco después de la sentencia del BVerfGE.[89] La nueva versión del §100g StPO comprende también los deberes del proveedor de internet,[90] quienes, en consecuencia, se encuentran obligados a almacenar la información y a transferirla a los funcionarios encargados de la persecución penal.[91]

La versión legislativa que entró en vigencia el 2008 fue modificada el 16 de octubre de 2015. La nueva ley sobre plazo para almacenamiento de datos formula algunas precisiones e incorpora específicamente los datos de posicionamiento (artículo 113b TKG). Entre los principales fundamentos de índole jurídica para la reforma se encuentra la sentencia de la EuGH en los casos C-293/12 y C-495/12, además de la necesidad de introducir a los datos de posicionamiento.

Los presupuestos formales para el acceso a la información alojada por el proveedor de internet surgen del §100g párr. 2 con relación a los §100b párr. 1-4 StPO y §113a/b TKG. El acceso al proveedor rige también para las medidas de acceso encubierto. Los nuevos presupuestos del §100g StPO se presentan de la siguiente manera:

a. Delito con significado relevante

La fórmula "delito con significado relevante" prevista en el §100g StPO resulta del derecho policial y fue empleado en el ámbito procesal con la introducción en el StPO del agente encubierto,[92] en el marco del catálogo general del "rastrillaje

---

números de llamadas u otros números de las conexiones que se utilizaron para llamar, o las que han sido llamadas, así como los cambios de cada una de las conexiones empleadas, o su nueva utilización, 2. La fecha y horario del comienzo y fin de la comunicación con datos sobre la zona horaria, 3. Datos sobre el servicio empleado, cuando en el marco de un servicio telefónico han podido ser utilizados diferentes servicios, 4. En el caso de servicios de telefonía móvil además, a) la identificación internacional de los participantes móviles para la conexión telefónica llamada y que es utilizada para llamar, b) la identificación internacional del dispositivo que llama y que es llamado, c) La fecha y el horario de la primera activación del servicio bajo denominación de la zona horaria, cuando el servicio ha sido pre-pagado (...) 5. En el caso de servicios de telefonía por internet también las direcciones de protocolo de internet de las conexiones que fueron empleadas para llamar y que fueron llamadas, y las identificaciones de los usuarios. (…); (5) El contenido de la comunicación, los datos sobre los sitios de internet solicitados y los datos de los servicios del correo electrónico no pueden ser almacenados con fundamento en esta disposición.

[89] Boletín Oficial alemán: BGBl. I p. 272.

[90] HORNUNG (2007), p. XIII.

[91] Conf. §§113a, y 113b StPO versión vigente hasta 2015, ver: KLESCZEWSKI (2008), S. 26; ECKHARDT (2007), p. 336.

[92] §110a, Párr. 1 S. 1.StPO.

electrónico",[93] así como también para el análisis de ácido desoxirribonucleico ("ADN").[94] Actualmente, la fórmula se encuentra en no menos de doce disposiciones del StPO,[95] y se relaciona tanto con delitos como también con contravenciones.[96]

La fórmula es parte componente del StPO desde la última versión del §100g StPO a la que se le agregan los delitos del segundo párrafo del §100a StPO. En suma, el §100g StPO incorpora una disposición orientada al caso particular y, además, un catálogo propio de delitos.[97] El catálogo de hechos comprende los delitos del §100a StPO segundo párrafo y en los delitos previstos en el nuevo §100g StPO, que consiste en un conglomerado de ochenta delitos e involucra también hechos imprudentes, previstos en normas complementarias del código penal "nuclear".[98] La fórmula "delito con significado relevante" comprende también a la tentativa punible y a los hechos preparatorios.[99]

El legislador ha renunciado solo en algunos casos a la fórmula cuando ya existe un catálogo expreso de delitos[100] y la limita habitualmente con el requerimiento de especial relevancia del bien jurídico, o el especial interés público en la persecución penal.[101]

La nueva categoría también coincide, en algunos casos, con otras ya existentes como la de "delitos especialmente graves".[102] Ambas fórmulas conducen, sin embargo, a que el examen de los presupuestos dependa de una ponderación de acuerdo con cada caso[103] lo que carece, en los hechos, de una función conceptual delimitadora real.[104]

b. Hechos cometidos a través de un medio de telecomunicación

El requerimiento de que el hecho sea cometido por un medio de telecomunicación resulta de la reforma de 2008 y se mantiene en el nuevo §100g

---

93 §98 a StPO.
94 §81a, Párr. 1 StPO, ver: WELP (2002), p. 538.
95 RIEß (2004), p. 623.
96 BverfGE 103, 21, 34, WELP (2002), p. 539. La referencia a los "delitos con significado relevante" previstos en la ley fue considerado por el BGH en 1996 conforme a derecho ("*Hörfallenentscheidung*"): RIEß (2004), p. 624.
97 WELP (2002), p. 539.
98 WELP (2002), p. 540. Esos requerimientos son suficientes para, por ejemplo, un robo con armas, o una estafa, defraudación, etcétera: WOLLWEBER (2002), p. 1554.
99 WELP (2002), p. 539.
100 RIEß (2004), p. 623.
101 PAEFFGEN (2001), p. 1304.
102 Por ejemplo: §100c I Nr. 1 StPO.
103 WELP (2002), p. 540; KLESCZEWSKI (2008), p. 28.
104 RIEß (2004), p. 623.

StPO (1 párrafo, núm. 2). Un delito es cometido a través de un medio de telecomunicación cuando, por ejemplo, es perpetrado con ayuda de un teléfono, un fax o de un ordenador conectado a la red, incluso cuando el medio es utilizado por un partícipe en el hecho.[105] De acuerdo con lo anterior, el §100g StPO es aplicable cuando un coautor desvía la atención del titular de un comercio por medio de una llamada telefónica, para que su cómplice pueda extraer los objetos no vigilados al mismo tiempo.[106]

El requerimiento de que el hecho sea cometido a través de un medio de comunicación tampoco tiene función delimitadora.[107] Tendría sentido en delitos como el *hacking,*[108] o el envío de virus informáticos,[109] pero no con otros delitos como, por ejemplo, una estafa cometida a través del empleo de medios de telecomunicación.[110] Si bien este requerimiento pretende limitar las potestades del §100g StPO[111] carece de tenor limitador.

Aquí se vuelve a hacer evidente un problema estructural en la doctrina en materia de criminalidad informática: la falta de concepto delimitador que permita establecer una distinción de esa área de conocimiento con otras. Por otra parte, también se evidencian problemas teóricos serios al examinar el resultado de la interacción de las disposiciones de la parte general del código penal alemán con disposiciones especiales. Faltan, pues, hipótesis puente (*bridge hipótesis*) que permitan relacionar disposiciones especiales o de derecho penal accesorio (Nebenstrafrecht) con el sistema conceptual de la parte general, y constituir un sistema o subsistema con propiedades específicas que fundamenten la especialidad de la investigación.

c. Personas obligadas a transferir la información

La transferencia de información en el proceso penal no es nueva en la legislación alemana. Ya el §12 FAG de 1928 preveía la transferencia de información a las autoridades encargadas de la persecución penal. El §12 FAG autorizaba a los jueces o a los fiscales, en caso de peligro en la demora, a requerir datos relacionados con la comunicación a los prestadores de servicios postales, cuando la información estaba dirigida a los acusados o cuando se trata de hechos sobre los cuales se puede decir que se dirigían al acusado y que la información era importante para la investigación.[112]

---

105 WELP (2002), p. 540.
106 WOLLWEBER (2002), p. 1554.
107 KLESCZEWSKI (2008), p. 28.
108 §302a StPO.
109 §§303a, 303b StGB.
110 WELP (2002), p. 540.
111 KORGE (2009), p. 89.
112 ZÖLLER (2007), p. 393.

La nueva versión del §100g, párrafo 3 StPO obliga a los prestadores de servicios de comunicación (entre otros, a los proveedores de servicios de internet) de una manera similar.[113] Todos los prestadores de servicios de comunicación están obligados a suministrar información.[114] Además, la nueva versión del §100g StPO mantiene el deber de los prestadores de servicios de congelar datos (*Quick-Freeze*), que consiste en capturar datos, almacenarlos y transferirlos de inmediato a los funcionarios encargados de la persecución penal.[115]

d. Datos como objeto de la medida

La norma central del §100g StPO es el nuevo §113b TKG (antes era el §113a, párrafo 2 TKG), que prevé un extenso catálogo de datos denominados "de tráfico". El §100g StPO se complementa con el artículo 96, párrafo 1 TKG, que también prevé una lista no taxativa de datos de tráfico. En la lista se encuentra el denominado número "PIN" que permite la activación de una tarjeta "SIM"[116] (Modulo de identificación del suscriptor) así como también el número "PUC" (o, "PUK") (código personal de desbloqueo), que permite desbloquear la tarjeta "SIM" en caso de que los números "PIN" (número de índice postal) hayan sido erróneamente introducidos.[117] El acceso a ambos datos permite naturalmente el acceso indirecto hacia datos de contenido. También están incluidos los datos sobre el lugar, tipo y forma de pago, la cantidad y la cualidad de los datos recibidos y enviados, el comienzo y la finalización de las llamadas, la duración de la comunicación y el número de protocolos de internet, en el caso de que se hiciera uso de servicios de telefonía vía internet.[118] Lo mismo rige para los prestadores de servicios de *e-mail*.[119]

La versión anterior §113b TKG preveía explícitamente que los datos no solo debían ser empleados para la persecución penal, sino también para la defensa frente a riesgos graves que afronta la seguridad pública y para cumplir con los fines de los servicios secretos.[120] Esta última prescripción prevista en el §113b TKG ha sido declarada inconstitucional por parte del BVerfGE[121] y no ha sido, por ende,

---

[113] El §3 Nr. 24 TKG define a los servicios de la comunicación como aquellos prestadores que lucran por la prestación de servicios que consisten principalmente en la transferencia de señales sobre una red de telecomunicación, especialmente en una red radioeléctrica. En consecuencia, los prestadores de servicios de una red LAN abierta están comprendidos en el deber de almacenamiento: HORNUNG (2007), p. XIII.

[114] §100g StPO como los artículos 16/7 de la Convención de Budapest.

[115] §113 a TKG y EU-2006/24/EG.

[116] Antes considerado como "dato de contrato" en el sentido del §§113 Párr. 1 oración 2 TKG en función del §§161 Párr. 1, 163 oración 1 StPO.

[117] §96 I Nr. I TKG en función del §100g StPO; KORN (2009), p. 120. ZÖLLER (2007), p. 399.

[118] KORN (2009), p. 120; PUSCHKE/SINGELSTEIN (2008), p. 117.

[119] §113a II TKG.

[120] PUSCHKE/SINGELSTEIN (2008), p. 117.

[121] BverfGE, sentencia del 2 de marzo de 2010 - 1 BvR 256/08, Nr. 309.

incorporada de nuevo por la ley de reformas.

En lo que respecta a las señales que envía el teléfono cuando está activado, y a los datos de posicionamiento que indica, la activación del teléfono móvil señala que este tiene disponibilidad para la comunicación, lo cual no significa que haya efectivamente una comunicación: es el dispositivo el que indica la disponibilidad para la comunicarse, no la persona.[122] El BverfGE confunde disponibilidad con comunicación en sí misma, para excluir del ámbito de la protección de la garantía que protege el secreto de las comunicaciones a los datos de posicionamiento, con el argumento de que falta comunicación.[123] En ese sentido, la nueva legislación incorpora, sin embargo, la jurisprudencia del BVerfGE y, por lo tanto, agrega a estos datos en el ámbito de la protección del secreto de las comunicaciones (artículo 6 de la reciente ley de reformas, lo que desde el punto de vista de la división de poderes resulta, sin embargo, dudoso).

El §100g StPO primer párrafo prevé que también se deben recolectar los datos previstos en el §96 TKG que se complementan con los datos previstos en la nueva versión del §113b TKG. Entre ellos se encuentran los números de teléfono de aquellos que pretendieron comunicarse o con quienes la persona investigada se pretendió comunicar, así como el número de identificación local e internacional de los aparatos involucrados ("IMSI" e "IMEI").[124] Dicha posibilidad de investigar datos de personas vinculadas con el sospechoso se denomina "búsqueda selectiva orientada" (Zielwahlsuche, vía IMSI *Catcher,* dispositivo de captura de la identidad internacional del suscriptor móvil).[125]

La versión anterior del §100g II StPO condicionaba la búsqueda selectiva orientada vía IMSI *Catcher* a una cláusula de subsidiariedad.[126] La búsqueda selectiva orientada debía ser ordenada solo cuando la investigación del hecho o del lugar en el que se encuentra el acusado no sería posible de otra manera o lo sería en forma muy dificultosa.[127] Tales requerimientos carecían de función limitadora:

---

122 NACHBAUR (2007), p. 337.

123 Ídem, p. 337.

124 La nueva posibilidad creada con la introducción en el 2002 del §100i StPO por medio de la cual se introdujeron los denominados "IMSI-*Catcher*" que permiten investigar los números de reconocimiento de los artefactos de comunicación ("IMEI": *International Mobile Equipment Identification*, e "IMSI": *International Mobile Subscriber Identity*), además de determinar la posición en la que se encuentran los aparatos móviles de comunicación, aparece vinculada por el BverfGE en su decisión del 22.8.2006 con el derecho a la autodeterminación informativa, y no con la garantía que protege el secreto de las comunicaciones según el artículo 10 GG: NACHBAUR (2007), p. 335.

125 La búsqueda selectiva de datos persigue que se produzca un rastrillaje de datos dirigido por el propio acusado y se extiende a personas no sospechosas: WELP (2002), p. 544. ZÖLLER (2007), p. 395. Para casos en los que el proveedor no procesa las llamadas entrantes, el §100g I StPO debe ser un fundamento suficiente para la investigación: PUSCHKE/SINGELSTEIN (2008), p. 115.

126 WOLLWEBER (2002), p. 1554/5.

127 *Ibid*, p. 1554/5.

El único límite real y actual era una ponderación de acuerdo con el principio de proporcionalidad de la injerencia.[128] Por otra parte, con motivo del deber de recolectar y almacenar datos tráfico en tiempo real según el §100g StPO, la "búsqueda selectiva orientada" había perdido actualmente importancia práctica en gran parte.[129] La nueva versión del §100g StPO mantiene la búsqueda selectiva orientada, aunque precisa los datos a recolectar a través del nuevo §113b y del 96 TKG.

La legislación orientada a la casuística está destinada a tener una vigencia temporal muy acotada, si se advierte que tampoco se ha elaborado una teoría puente que permita conformar un sistema conceptual entre la noción de dato (concepto que posiblemente provenga de la teoría de la información), con el sistema conceptual de la ley de telecomunicaciones. La definición de dato con la que opera el §268 StGB: "informaciones que pueden ser procesadas por un dispositivo de análisis de datos o que representan el resultado de tal procesamiento",[130] no solo es demasiado amplia y circular, sino que confunde información con dato, y el objeto del examen con el dispositivo de examen (¡dato es información que puede ser procesada o que es el resultado de un dispositivo que examina datos!), además de que no aporta nada nuevo. No hay hasta el momento un sistema conceptual integrador satisfactorio.

e. Límites temporales

Según la versión anterior del §100g StPO en función del §113a TKG se debía recolectar y conservar los datos en un plazo de seis meses. Los funcionarios encargados de la persecución penal pueden tener incluso acceso retroactivo a los datos dentro de ese período, entonces, la medida se extiende pues a los doce meses. El derecho vigente, de acuerdo con los §97, párrafo 4, y número 2 TKG en virtud del cual las personas afectadas podían solicitar la supresión, borrado o su anonimato, resultó abrogado en la nueva versión del §113a TKG en función del nuevo §100g StPO.[131]

La nueva versión del §100g StPO, en función del nuevo §113b TKG, redujo el plazo para almacenar datos a diez semanas en lo que respecta a la información mencionada en el primer y segundo párrafo del nuevo §113b TKG y, por cuatro semanas, respecto de los datos de posicionamiento. También prohíbe expresamente el almacenamiento de los datos de contenido (§113 TKG, 5.) (Véase *supra* "V 3.d. "datos como objeto de la medida" y nota al pie de página número 88). Si bien se redujeron sustancialmente los plazos previstos en la versión anterior del §100g StPO, se incrementó el catálogo de datos a recolectar.

---

[128] *Ibid*, p. 1554/5.

[129] PUSCHKE/SINGELSTEIN (2008), p. 115.

[130] Por ejemplo: HILGENDORF/THOMAS/VALERIUS (2005), p. 48, núm. márg. 168.

[131] KORN (2009), p. 120.

VI. Consideraciones finales

La jurisprudencia anterior del BVerfGE referida al acceso a los datos almacenados en los servidores de correos electrónicos, partía de la base de que las personas vigiladas tienen el mismo dominio sobre el correo electrónico que sobre el correo postal. La jurisprudencia actual del BVerfGE, incluso luego de modificar su criterio, sigue equiparando los correos electrónicos al correo postal en la medida en que utiliza el criterio de "esfera de dominio",[132] proveniente de la comunicación postal tradicional.[133] Además, según ella, el derecho a la autodeterminación informativa pasa a depender de que la persona vigilada no adopte medidas para evitar el acceso a sus datos, cuando estos se encuentran en su esfera de dominio.[134]

La equiparación ilimitada abre la puerta para la aplicación de los §§94 y 97 StPO para la información alojada en los servidores de correos electrónicos y, al no existir comunicación, con la exclusión de la aplicación de la garantía que protege el secreto de las comunicaciones y, por ende, de los presupuestos procesales previstos en los §100a y siguientes del StPO[135] que, por definición, son más restringidos que los previstos en los §§94 y 97 StPO. No está claro hasta qué punto el artículo 6 de la reciente reforma, según el cual la nueva ley tiene repercusión en la garantía que protege el secreto de las comunicaciones tiene alguna importancia práctica, pues la determinación de la influencia de una legislación sobre las garantías no es tarea del legislador. Por otra parte, la incorporación en el §100g StPO (en relación con los §§113a y b de la TKG) de los datos de posicionamiento, sin que exista comunicación, debería ser un argumento en contra la aplicación de las disposiciones sobre secuestro de cosas (§§94 y 97) y por lo tanto, debería entenderse como "derogatoria" de la jurisprudencia que equipara los datos a las cosas materiales, para habilitar el secuestro.

En la medida en que la transferencia de información haya sido objeto de almacenamiento intermedio por el prestador de servicios de comunicación no es técnicamente viable el concepto de "esfera de dominio de los datos" por parte del particular.[136] El requerimiento de cierto dominio sobre datos no coincide con el fundamento del derecho a la autodeterminación informativa. No existe, hasta el momento, un examen de compatibilidad teórica entre el concepto de dominio y la ubicación física de los datos en el almacenamiento local del titular de los datos o en el almacenador de los servidores.

---

132 SCHLEGEL (2007), p. 46/7; KUTSCHA/THOMÉ (2013), p. 63.

133 BRÜNUNG (2006), p. 240.

134 SCHLENGEL (2007), p. 50/1.

135 *Ibid*, p. 49.

136 El reconocimiento del almacenamiento intermedio se encuentra en los §113a TKG, §100 g StPO de existir una orden judicial, así como en la directriz EU-2006/24/EG y artículo 16/7 de la Convención sobre Ciberdelincuencia. No es técnicamente posible hablar de "dominio". Sobre las particularidades técnicas: HOLTKAMP (2002), p. 43.

Por otra parte, la puesta en práctica de directriz EU-2006/24/EG se fundamenta, en última instancia, en el artículo 95 EGV del Convenio Europeo que, en lo sustancial, parece tener un carácter vinculante mayor que toda la Convención sobre Ciberdelincuencia. El legislador alemán pretende luchar contra el terrorismo, ampliando las potestades de injerencia sobre personas, incluso sin sospecha previa.[137] El fundamento de la reforma procede de un órgano de la Unión Europea actuando en exceso de competencia.[138] En ese sentido, el pronunciamiento del EuGH de abril de 2014 y del BVerfGE del 2 de marzo de 2010, evidencian los déficits de legalidad en la fundamentación de la génesis de las directrices y de la legislación que entró en vigencia como consecuencia de ello (déficit genético de la legislación).

El §100g StPO autoriza el ingreso intensivo a los datos de tráfico de las redes de acceso público en Alemania[139] tales datos pueden ser, por ejemplo, objeto de una búsqueda selectiva orientada de datos y, por ende, estar bajo un control procesal constante.[140] Esta medida está aún vigente en la medida en que el catálogo de delitos al que hace referencia el nuevo §100g StPO carece de efecto limitador y se fundamenta en los actos preparatorios. La amplitud de la injerencia también se confirma con el enfriamiento de datos en tiempo real y con la posibilidad de utilizar esos datos en un proceso penal. El §100g StPO amplía considerablemente la cantidad de datos a almacenar e incrementa las posibilidades de que los datos personales sean indebidamente manipulados, al mismo tiempo que se extiende a datos de personas no sospechosas.[141]

La modificación del §100g StPO tiene influencia en otras medidas procesales como, por ejemplo, las previstas en los §100a, b e i, StPO.[142] Para la aplicación del §100g StPO no se necesita ninguna comunicación real, sino simplemente la posibilidad de que exista una comunicación, lo que se vuelve explícito con la incorporación del criterio del BVerfGE (ver *supra* núm. 3, lit. "d".) al permitir la recolección de datos de posicionamiento.

Por otra parte el §100g StPO, a pesar de que la incorporación de datos no es precisa y colisiona, por ende, contra el mandato de determinación previsto en el artículo 103, párrafo 2 GG, especialmente porque la referencia a los §§96 y 113 TKG y al catálogo de delitos no es limitadora, lo que se confirma con la referencia a otras fórmulas como: "delito con significado relevante" y "consideración del caso particular".

---

137 Art. 19 párr. 1 p. 2 GG, arts. 72 y 74 párr. 1 Nr. 1 GG: ZÖLLER (2007), p. 409.
138 *Ibid*, p. 410 y 415.
139 Cuyo número estima que ronda los 100 millones anuales: WELP (2002), p. 545.
140 WELP (2002), p. 545.
141 PUSCHKE/SINGELSTEIN (2008), p.118.
142 PUSCHKE/SINGELSTEIN (2008), p.119.

Además el almacenamiento y registro de datos según el §100g StPO carece de límites, porque para su empleo se requiere únicamente contar con una sospecha de delito[143] y, sobre todo, porque el procedimiento "*Quick Freeze*", que se mantiene en el nuevo §100g StPO (ver §100g StPO, primer párrafo, núm. 2), es menos incisivo que el almacenamiento genérico de datos previsto en la directriz 2006/24/EG, legitimado por el StPO.[144] Por su parte, la búsqueda selectiva de datos vía IMSI *Catcher* es una de las formas más intensivas de rastrillaje informático.[145] Sus límites aún no están claros, ni siquiera con las precisiones en torno a los datos de los §§113b y 96 TKG, pues comprenden casi todas las posibilidades de cometer delitos con el uso de un medio de telecomunicación,[146] además de que incrementa el arsenal de posibilidades de recolección y captura de datos prevista en el §100 StPO.[147] La medida excede, por ende, cualquier proporción legitima[148].

Este argumento deja en evidencia que las hipótesis que habilitan la vigilancia electrónica no son el resultado del examen de la interacción de dos sistemas conceptuales: por un lado, el sistema conceptual que surge de la relación entre los conceptos de información, dato y comunicación y, por el otro, las regulaciones del StGB, StPO, TKG y BDSG.

La extensión temporal prevista en la versión anterior del §100g StPO era desproporcionada, especialmente porque se podía acceder a los datos en forma retroactiva durante seis meses luego que los datos fueran recolectados.[149] La nueva versión del §100g StPO distingue los datos a recolectar y redujo el plazo según se trata de los datos previstos en los párrafos 2 y 3 del §113b TKG (diez semanas) y los datos de posicionamiento (cuatro semanas). Sin embargo, la dimensión temporal del problema puede indicar el desarrollo y la aceleración de técnicas de procesamiento de datos, con lo cual solamente reconoce que el estado tiene una capacidad técnica más avanzada con respecto a 2008.

143 PUSCHKE/SINGELSTEIN (2008), p.118; WELP (2002), p. 545.
144 DERKSEN (2011), S. 16
145 WELP (2002), p. 545.
146 WELP (2002), p. 546.
147 KLESCZEWSKI (2008), p. 30.
148 WELP (2002), p. 546.
149 DERKSEN (2011), p. 16

BIBLIOGRAFÍA:

- BREYER, Patrick (2007): "Rechtsprobleme der Richtlinie 2006*24/EG zur Vorratsdatenspeicherung und ihrer Umsetzung in Deutschland", en Revista: Strafverteidiger (StV) 4/2007, Luchterhand, Köln, p. 215.
- BRÜNUNG, Janique (2006): "Der Zugriff auf die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Kommunikationsdaten. Zugleich eine Anmerkung zum Urteil des 2. Senats des Bundesverfassungsgerichts vom 2. März 2006- 2 BvR 2099/04", en Revista: Zeitschrift für internationales Strafrecht (ZIS 6/2006), p. 240.
- BUNGE, Mario (1987): *Kausalität, Geschichte und Probleme*, J.C.B. Mohr, Tübingen, 1987, p. 26.
  _____ (2001): "Scientific Realism" en obra colectiva: *Selected Essays of Mario Bunge*, Martin Mahner, Prometheus Books, New York, p. 82.
- DERKSEN, Roland (2011): *Zur Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta*, 25. Februar: http://www.vorratsdatenspeicherung.de/images/ rechtsgutachten_grundrechtecharta.pdf, p. 8.
- ECKHARDT, Jens (2007): "Die Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen", en Revista: *Computer und Recht* (CR), p. 336.
- GERCKE, Marco (2004): "Die Cybercrime Konvention des Europarates. Bedeutung und Tragweite ihres völkerrechtlichen Einflusses auf das Straf- und Strafverfahrensrecht in Deutschland", en Revista *Computer und Recht* (CR), p. 782.
- GRAFE, Adina (2007): "Die Auskunftserteilung über Verkehrsdaten nach §§100g, 100h StPO-Staatliche Kontrolle unter Mitwirkung Privater, Inaugural-Dissertation zur Erlangung des Grades eines Doktors der Rechte des Fachbereichs Rechtswissenschaft an der Albert-Ludwigs-Universität" in Freiburg im Breisgau, Dezember, disponible http://www.freidok.uni-freiburg.de/volltexte/6085/pdf/Verkehrsdaten.pdf, p. 23.
- HILGENDORF, Eric/THOMAS, Frak/VALERIUS, Brian (2005): *Computer und Internetstrafrecht. Ein Grundriss*, Springer, Berlin, Heidelberg, New York, p. 48, núm. márg. 168.
- HOLTKAMP, Heiko (2002): *Einführung in TCP/IP, AG Rechnernetze und Verteilte Systeme Technische Fakultät*, Universität Bielefeld, p. 43.
- HORNUNG, Gerrit (2007): "Wireless und speicherpflichtig? Die Vorratsdatenspeicherung und der Betrieb von W-Lan-Systemen", en Revista: *Multimedia und Recht* (MMR) 12/2007, p. XIII.
- KLESCZEWSKI, Diethelm (2008): "Kritik der Vorratsdatenspeicherung", en obra colectiva: *FS-Fezer*, Wesslau- Wohlers, Hrgs., De Gruyter, Berlin, p. 24.
- KORN, Jana (2009): "Der strafprozessuale Zugriff auf Verkehrsdaten nach §100g StPO", en Revista: *Höchst Richterliche Rechtsprechung im Strafrecht* (HRRS) 3/2009, Hamburg, p. 114.
- KORGE, Tobias (2009): *Die Beschlagnahme elektronisch gespeicherter Daten bei privaten Trägern von Berufsgeheimnissen*, Springer, Berlin, Heidelberg, p. 89.
- KUTSCHA, Martin/THOMÉ, Sarah (2013): *Grundrechtschutz im Internet?*, Nomos, Baden Baden, p. 15.
- NACHBAUR, Andreas (2007): "Standortfestellung und Art. 10 GG- Der Kammerbeschluss des BverfGE zum Einsatz des "IMSI-Catchers"", en Revista *Neue Juristische Wochenzeitschrift* (NJW), Beck, München-Frankfurt, p. 337.
- PAEFFGEN, Hans-Ullrich (2001): "Überlegungen zu einer Reform des Rechts der Überwachung der Telekommunikation", en obra colectiva: *FS-Roxin*, De Gruyter, Berlin-New York, p. 1304.
- PUSCHKE, Jens/SINGELSTEIN, Tobias (2008): "Telekommunikationsüberwachung, Vorratsdatenspeicherung und (sonstige) heimliche Ermittlungsmaßnahmen der StPO nach der Neuregelung zum 1.1.2008", en Revista: *Neue Juristische Wochenzeitschrift* (NJW), Beck, München-Frankfurt, S. 114.

- RIEß, Peter (2004): "Die Straftat von erheblicher Bedeutung" als Eingriffsvorausetzung Versuch einer Inhaltsbestimmung, en Revista: *Goltdammer's Archiv für Strafrecht* (GA), R.V. Decker, Heidelberg, p. 623.
- SACHS, Michael (2014): *Grundgesetz Kommentar*, 7. Aufl., Beck, München, p. 498, Nr. 8.
- SCHENKE, Ralf (2000): "Präventive Überwachung der Telekommunikation", en revista: *Archiv de öffentlichen Rechts*, J.C.B. Mohr (Paul Siebeck), Tübingen, p. 19.
- SCHLEGEL, Stephan (2007): ""Beschlagnahme" von E-MailVerkehr beim Provider", en Revista: *Höchst Richterliche Rechtsprechung im Strafrecht* (HRRS), Hamburg, p. 46/7.
- WELP, Jürgen (1994): "Anmerkung zu BGH, 24.02.1994- 4StR 317/93", en Revista: *Neue Zeitschrift für Strafrecht* (NStZ), C.H. Beck, München, Frankfurt, p. 295.
  _____ (2002): "Verbindungsdaten. Zur Reform des Auskunftsrechts (§§100g, 100h StPO)", en Revista *Goldtdammer's Archiv für Strafrecht* (GA), Beck, München- Frankfurt, p. 539.
- WESTPHAL, Dietrich (2006): "Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten- Brüsseler Stellungnahme zum Verhältnis von Freiheit und Sicherheit in der „Post-911-Informationsgesellschaft"", en Revista: *Europa und Recht* (EuR), Nomos, Baden-Baden, p. 712.
- WOLLWEBER, Harald (2002): "Verbindungsdaten der Telekommunikation im Visier der Strafverfolgungsbehörden", en Revista: *Neue Juristische Wochenzeitschrift* (NJW), Beck, München-Frankfurt, S. 1554.
- ZÖLLER, Mark A. (2007): "Vorratsdatenspeicherung zwischen nationaler und europäischer Strafverfolgung", en Revista: *Goldtdammer's Archiv für Strafrecht* (GA), Beck, München-Frankfurt, p. 408.