REVISTA
DE ESTUDIOS DE LA JUSTICIA

NÚM. 27 (2017) • PÁGS. 61-79 • DOI 10.5354/0718-4735.2017.47961
RECIBIDO: 27/12/16 • APROBADO: 31/7/17 • PUBLICADO: 30/12/2017

DOCTRINA

Intercepción de metadatos de comunicaciones por teléfonos móviles. El IMSI-Catcher y su regulación en el ordenamiento procesal penal alemán

Interception of communications metadata by mobile phones. IMSI-Catcher and his regulation on the German criminal procedure

Darío Nicolás Rolón

Friedrich Alexander Universität Erlangen-Nürnberg, Alemania

RESUMEN Este artículo se ocupa de la legislación del denominado IMSI-Catcher bajo la Ley Alemana de Procedimientos Penales (§100i StPO), y la Ley Constitucional Alemana. El IMSI-Catcher es un dispositivo técnico diseñado por la firma Rhode and Schwarz en 1996 para la búsqueda, identificación y almacenamiento de la identidad internacional móvil de suscriptor (IMSI), para determinar la identidad internacional del equipo móvil (IMEI) y para localizar a los usuarios del dispositivo móvil conectado al sistema de red global de comunicación móvil (en sus siglas en inglés «GMS»). El marco legal del IMSI-Catcher en Alemania ha sido durante mucho tiempo materia de discusión sobre la disposición legal específica bajo la cual el dispositivo debería ser utilizado. De hecho, antes de la disposición legal actual del IMSI-Catcher bajo el §100i StPO, el dispotivo ha sido empleado en numerosas oportunidades con el argumento de que el uso del dispositivo se fundamenta en ciertas disposiciones generales sobre el uso de evidencia (§§161 y 163 StPO) o en otras disposiciones legales ya existentes relativas al secreto de las comunicaciones (§100 «a», «b» o «c» StPO). Esta situación legislativa anárquica habilitó a la policía federal y local, al servicio secreto y a los funcionarios a cargo de la persecución penal emplear el IMSI-Catcher no solo en casos de terrorismo, sino también en otros casos de naturaleza penal. Debido al número de reformas relacionadas muy estrechamente con otras prescripciones legales próximas a la regulación del IMSI-Catcher, por ejemplo, §100g StPO, y algunos casos recientes en la jurisprudencia de la Corte Constitucional Alemana, el análisis legal del §100i StPO se ha modificado. El artículo consiste en un análisis legal de las modificaciones mencionadas.

PALABRAS CLAVE IMSI-Catcher, secreto de las comunicaciones, comunicaciones móviles, derecho a la autodeterminación informativa, vigilancia de las telecomunicaciones, libertad probatoria.

ABSTRACT This article focuses on the enactment of the so called IMSI-Catcher under to the German Procedural Law (§100i StPO), and Constitutional Law. The IMSI-Catcher is a technical device designed by the Firm Rhode and Schwarz in 1996 for searching, identifying, and gathering the international mobile subscriber identity (IMSI), the international mobile equipment identity (IMEI), and also for localizing users of a mobile telephone device connected the Network Global System for Mobile Communication (GMS). The legal framework of the IMSI-Catcher in Germany has been for a long time issue of hard debates around the specific legal provision under which the device shall be employed. In fact, before the current enactment of the IMSI-Catcher under §100i StPO, the device has been employed several times according the argument that the use of IMSI-Catcher lies on some general clauses of evidence (§§161 and 163 StPO) or on already enacted provisions about secrecy of communications (§100 «a», «b» or «c» StPO). This anarchic legal situation enabled the federal and local police, the secret service, and criminal prosecutors to employ the IMSI-Catcher not only in cases of terrorism, but also in a large set of criminal cases. Due to a set of reforms related to others very close connected legal prescriptions, e.g. §100g StPO, and some recent cases in the jurisprudence of the German Constitutional Supreme Court the legal analysis of §100i StPO has been modified. This article consists on a legal analysis of the before mentioned modifications.

KEYWORDS IMSI-Catcher, secrecy of communications, movil communication, right to informative self-determination, surveillance of telecommunications, evidence freedom.

Introducción

El dispositivo técnico denominado IMSI-Catcher fue introducido por el legislador en el ordenamiento procesal penal alemán (StPO, por sus siglas en alemán en el §100i StPO[1] el 6 de agosto de 2002 (BGBl. I 2002), y entró en vigencia el 14 de agosto de 2002. El IMSI-Catcher permite determinar los números IMEI/IMSI de un dispositivo móvil, así como también la identificación del lugar donde se encuentra la persona inculpada, y la escucha en tiempo real de sus conversaciones.

1. §100i StPO: «1) Si determinados hechos fundamentan la sospecha de que alguien como autor o partícipe de un delito que también en el caso concreto tiene significativa relevancia, especialmente un delito previsto en el §100a párr. 2, en los casos en los que la tentativa también es punible, ha intentado su comisión, o lo ha preparado mediante la comisión de otro delito, se puede averiguar por medios técnicos: 1. El número de aparato de telefonía móvil y el número de tarjeta de la carta allí inserta, así como: 2. La localización del dispositivo móvil, siempre que sea necesario para la averiguación del hecho o la investigación de la localización del inculpado. 2) Datos relacionados con las personas pueden ser recolectados a través de tales medidas cuando es inevitable por razones técnicas para lograr la finalidad del párrafo 1. Los datos no pueden ser utilizados más allá de la averiguación del número de dispositivo y de tarjeta, y deben ser eliminados de inmediato luego de la conclusión de la medida. 3) §100a párr. 2 y §100b párr. 1 oración 1 a 3, párr. 2 oración 1 y párr. 4 oración 1 rigen correspondientemente. La orden tiene una duración de seis meses. Está permitida una prórroga de no más de seis meses, siempre que los presupuestos mencionados en el párrafo 1 subsistan». Todas las traducciones son nuestras.

Si bien la medida técnica ha sido empleada con independencia y a falta de una disposición legislativa expresa, luego de transcurridos más de catorce años desde la incorporación del dispositivo en la legislación alemana, y más de veinte años desde la existencia del dispositivo, el desarrollo de la tecnología, y, como consecuencia de ello, las reformas procesales ocurridas en otros ámbitos normativos próximos, como, por ejemplo, la recolección de datos prevista en el §100g StPO, así como también diversas interpretaciones jurisprudenciales, y sentencias del Tribunal Federal Constitucional alemán (Bundes Verfasung Gericht, BverfG), han tenido una notable repercusión en el alcance de la interpretación del texto del §100i StPO, por lo que deviene imprescindible examinar de cerca la extensión de las disposiciones contenidas en el §100i StPO.

Una razón adicional para el examen radica en que el legislador alemán, mediante el §100i StPO, decidió regular el empleo de un medio técnico para la obtención de datos relacionados con la comunicación (en algunas ocasiones también llamados «metadatos»), sin detenerse, como en la mayoría de las oportunidades, en las formas específicas para la captura de datos en tiempo real, o las escuchas telefónicas, con independencia del medio empleado.

Fundamentos del IMSI-Catcher

Descripción técnica del IMSI-Catcher

El IMSI-Catcher es un dispositivo que ha sido puesto a prueba en diciembre de 1996, bajo el modelo GA 090, luego perfeccionado bajo el modelo GA 900, por la empresa Rhode and Schwarz, y consta de una consola de control, dispositivos de medición y una antena. El IMSI-Catcher modelo GA 900 tiene tres funciones principales: la determinación de los números IMSI[2]/IMEI[3] de dispositivos móviles, la identificación del lugar de la celda radioeléctrica en la que se encuentra posicionado el dispositivo[4]

2. El número IMSI (International Mobile Subscriber Identity) es una identificación compuesta de quince números, cuyas cinco primeras cifras permiten identifica el código de país, y la empresa de red, que, en segunda instancia, permiten la identidad del usuario registrada ante el prestador de servicios de telefonía móvil, mientras que con ayuda del resto de los números se puede identificar la identidad del usuario y el número de teléfono. El número IMSI se almacena en la tarjeta SIM (Subscriber Identity Module) del teléfono móvil. Cada usuario de la red GMS recibe un número único en todo el mundo. Sobre esto, véase Harnisch y Pohlman, (2009: 203).

3. El número IMEI (International Mobile Equipment Identity) también es un número único que identifica el número de dispositivo móvil, y consiste, al igual que el número IMSI, en quince dígitos. Véase Harnisch y Pohlman (2009: 203).

4. Una celda radioeléctrica es la unidad mínima del espectro de ondas radioeléctricas. El tamaño de una celda se determina según el ámbito que cubre su estación base (torre de envío de señales), que puede ir desde algunos metros hasta varios kilómetros, dependiendo de la densidad poblacional. Véase Harnisch y Pohlman (2009: 203).

cuando el teléfono móvil está activado (lo que incluye el estado *stand by*), y la escucha de las conversaciones en tiempo real (Wolter, 2010: 304; Bode, 2012: 410).

Funcionamiento

El IMSI-Catcher simula una onda electromagnética en la estación base más próxima, que habitualmente corresponde con el sitio del usuario a vigilar. Debido a que las ondas de las antenas de envío de señales generalmente se superponen, el dispositivo busca el teléfono móvil con señal más potente (Harnisch y Pohlman, 2009: 203), y envía una señal aun más fuerte, lo que permite captar por un instante las transmisiones de todos los dispositivos móviles de la zona, y obtener el número IMSI, para luego reenviarlos directamente hacia la antena base. El aparato también identifica el número IMEI de los dispositivos a vigilar para identificar al usuario, con independencia de los cambios en la tarjeta móvil que utilice y de las modificaciones en el número IMSI (Harnisch y Pohlman, 2009: 204).

Además, el IMSI-Catcher identifica la ubicación geográfica de la tarjeta SIM.[5] La precisión de la localización, en virtud de los datos GPS (Global Positioning System), depende del tamaño la celda en la que se encuentra la persona a identificar (Harnisch y Pohlman, 2009: 204). Para ello, el artefacto identifica la señal más baja que se emite desde la celda de onda en la que se encuentra el teléfono, con una precisión aproximada de un radio de treinta metros (Harnisch y Pohlman, 2009: 203; Gercke, 2002a). No es clara la relevancia práctica de esta última función, en virtud de la vigencia de otros dispositivos más eficaces, como, por ejemplo, el SMS silencioso.

La determinación de los números IMSI/IMEI y la localización del usuario del teléfono móvil permiten luego que los funcionarios a cargo de la persecución penal recurran a otras medidas de prueba, como, por ejemplo, la vigilancia de las telecomunicaciones (§100a/b StPO), o la recolección de datos de tráfico (§100g StPO), y la determinación de la identidad del usuario de un servicio de telefonía móvil (Eschelbach, 2014: 496).

Efectos técnicos colaterales

El empleo del IMSI-Catcher lleva aparejada la desactivación por un instante del funcionamiento de los otros dispositivos móviles, cuya señal resulta también atraída por la señal simulada por el IMSI-Catcher. Quedan inhabilitadas, por ende, las funciones de voz y mensajes de texto, y los servicios de emergencia de los dispositivos móviles afectados por la medida (Harnisch y Pohlman, 2009: 204). Si bien el Gobierno Fede-

5. La estación de onda del prestador de servicios busca, en virtud de los denominados Mobile Switching Cente (MSC), esas señales constantes de los teléfonos (cf. Gercke, 2002a: 30). Identificar el número de tarjeta SIM presupone determinar la localización de la persona (Harnisch y Pohlman, 2009: 204).

ral alemán indica que la interrupción puede durar hasta diez segundos, los propios prestadores técnicos del servicio mencionan un lapso de varios minutos. El empleo del IMSI-Catcher puede saturar el funcionamiento de la antena base, y afectarla en forma duradera (Harnisch y Pohlman, 2009: 205).

Examen del §100i StPO

Fundamentos para el empleo del IMSI-Catcher antes de la reforma del §100i StPO

Antes de la regulación expresa del IMSI-Catcher en el §100i StPO en 2002, se discutía si su empleo ya estaba autorizado por las disposiciones del StPO. Por ejemplo, el Gobierno Federal sostenía que los funcionarios a cargo de la persecución penal podían invocar los §§100a y ss. StPO, sobre intercepción de las comunicaciones electrónicas, en relación con el §161 StPO, que consiste en una cláusula general según la cual los funcionarios a cargo de la persecución penal pueden hacer investigaciones previas, para solicitar posteriormente la vigilancia electrónica.[6]

El Gobierno Federal sostenía que los §100a/b StPO, que regulan los presupuestos para la vigilancia de las comunicaciones, hacían mención de la posibilidad de vigilar comunicaciones entre determinados números telefónicos, y *otros números*. La referencia legal a «otros números» era el fundamento para sostener que los números IMSI/IMEI ya se encontraba previsto según el §100b párr. 2, oración 2 StPO. El §100a StPO permitía identificar los datos de posicionamiento, cuando el teléfono se encontraba en *stand-by*.[7] Sin embargo, el §100a StPO requiere la intervención de una empresa prestadora de servicios, a diferencia del empleo del IMSI-Catcher (Schäfer, 2004: 507).

En las recomendaciones del Parlamento alemán sobre el proyecto del Gobierno Federal también se citaba la interpretación del AG München de 2001, que sustentaba el empleo del IMSI-Catcher con fundamento en la versión anterior del §100c párr. 1 núm. 1 lit. «b» del StPO, que autorizaba al empleo de «otros medios técnicos» con fines de observación,[8] como, por ejemplo, las tomas fotográficas con finalidad de vigilancia (Gercke, 2002: 127). Sin embargo, el Parlamento alemán destacaba que el §100c StPO, no contemplaba en forma expresa el IMSI-Catcher, con lo que resultaba conveniente una regla expresa, especialmente porque la Ley Antiterrorista del 9 de

6. Respuesta del Gobierno Federal a una consulta realizada por representantes del partido FDP BT-Drucksache 14 6885.

7. Bundesrat-Empfehlung zu Entwurf der Bundesregierung 10.06.02, Drucksache 452/1/02, p. 3

8. Empfehlung des Bundesrates zum Entwurf der Bundesregierung 10.06.02, Drucksache 452/1/02, p. 3; se refiere a la decisión del AG München del 5 de septiembre de 2001, Gz. ER II Gs 9039/01; cf. Harnisch y Pohlan, 2009: 205.

enero de 2002 preveía en el §9 párrafo 4 BVerfSchG una regla detallada que podría tener repercusión en el ámbito procesal penal.[9] Esta argumentación es compatible con la que sostiene que el principio de reserva impedía el empleo del IMSI-Catcher con apoyo en esta regla (Schäfer, 2004: 507).

Asimismo, con fundamento en el estado de necesidad justificante del §34 del Código Penal alemán (StGB, por sus siglas en alemán), entre 1998 y 2001 se empleó el dispositivo un total de 35 veces (Harnisch y Pohlan, 2009: 206). Es dudoso que el §34 StGB pueda satisfacer completamente los requerimientos del principio de reserva constitucional aplicable al derecho procesal penal, al margen de que las causas de justificación regulan comportamientos de ciudadanos y no de oficinas estatales frente a peligros comunes (Harnisch y Pohlan, 2009: 206).

Para la doctrina dominante no existía ningún fundamento legal para utilizar el IMSI-Catcher antes de su regulación específica en el §100i StPO (Harnisch y Pohlan, 2009: 206). En ese mismo sentido el BverfG sostuvo en la sentencia del 22 de agosto de 2006, que el empleo del IMSI-Catcher no se encuentra comprendido por las disposiciones sobre vigilancia de las telecomunicaciones del §100i StPO, pues los datos a los que se refiere (IMSI/IMEI) no se refieren a la comunicación, ni a las circunstancias próximas a la comunicación estrictamente vinculadas con el contenido de la comunicación y, por lo tanto, no se aplica la garantía que protege el secreto de las comunicaciones.[10] La sentencia del BverfG motivó la reforma al §100i StPO y entró en vigencia a partir del 1 de enero de 2008.

Antecedentes de la versión actual del §100i StPO

Ya a partir de 1997 se formularon propuestas para prever reglas específicas sobre el uso del IMSI-Catcher. El Gobierno Federal se opuso inicialmente a la creación de una nueva regla hasta la presentación de otro nuevo proyecto formulado por el mismo gobierno, el 23 de noviembre de 2001, que tenía por objeto la modificación del ordenamiento procesal, especialmente los §§81 y ss. StPO, y que finalmente fue aprobado el 6 de agosto de 2002, y entró en vigencia, junto con la nueva versión del §100i StPO, el 14 de agosto de 2002 (Harnisch y Pohlan, 2009: 206).

Si bien la reforma del §100i StPO de 2002 no fue sustancial, a partir de entonces se impulsó una nueva reforma integral de las medidas de vigilancia. El proyecto de reforma presentado por el Gobierno Federal el 27 de junio de 2007 ante la necesidad de implementar la directriz 2006/24/EG comprendió una modificación a las reglas previstas en los §§100a y ss. StPO, entre ellos, el §100i StPO, donde se incorporaron nuevos presupuestos y se suprimieron algunos límites de la medida (Harnisch y Po-

9. Bundesrat-Empfehlung zu Entwurf der Bundesregierung 10.06.02, Drucksache 452/1/02, p. 3.
10. BVerfG 2 BvR 1345/03 - 22. August 2006 (-) [= HRRS 2006 Nr. 807], núm. márg.: 51, 55.

hlan, 2009: 206). Finalmente, el 1 de enero de 2008 se reformaron todas las medidas de vigilancia encubierta, y de vigilancia de las telecomunicaciones.

Presupuestos del §100i StPO

Antes de la reforma de 2008, la medida tenía como finalidad la obtención de una orden de vigilancia de las telecomunicaciones, y debía interpretarse en el marco de la recolección de datos de tráfico en los términos del §100g StPO, u otras medidas de vigilancia admisibles (Harnisch y Pohlan, 2009: 206). Estos presupuestos se suprimieron en la versión final que entró en vigencia el 1 de enero de 2008.

Según la nueva versión del §100i StPO, las medidas de mayor grado de injerencia no pueden sustentarse en el §100i StPO, sino que deben hacerlo conforme con los §§100a y ss. StPO, lo que no significa que exista subsidiariedad estricta entre el §100i StPO y las medidas del §100a y ss. StPO (Hilger, 2002: 557), pues el nuevo §100i StPO carece de cláusula de subsidiariedad, y no impide que pueda ser utilizado por las fuerzas policiales o el servicio secreto ante presuntos casos de terrorismo.[11]

Delito de significativa relevancia

La fórmula «delito de significativa relevancia» resulta del derecho policial y fue empleado en el ámbito procesal con la introducción en el StPO del agente encubierto,[12] en el marco del catálogo general del «rastrillaje electrónico»,[13] así como también para el análisis de ácido desoxirribonucleico (ADN).[14] La fórmula se encuentra en no menos de doce disposiciones del StPO (Rieß, 2004: 623) y se relaciona tanto con delitos como también con contravenciones.[15] El catálogo de hechos comprende los delitos del §100a StPO segundo párrafo y en los delitos previsto en el nuevo §100g StPO, que consiste en un conjunto de ochenta delitos e involucra también hechos imprudentes, previstos en normas complementarias del código penal «nuclear» (Welp, 2002: 540).[16] La fórmula «delito de significativa relevancia» comprende también a la tentativa punible y a los hechos preparatorios (Welp, 2002: 539).

---

11. En el ámbito preventivo: §25 a párrafo 2 ASOG, §33 b párr. 3 BdgPolG, §34a párr. 2 BayPAG, §33 párr. 1 BremPolG, §23a párr. 6 BWPolG, §10b párr. 3 HmbDVPolG, §15a párr. 3 HSOG, §185a párr. 3 LvwG SH, §33b párr. 1 Nds.SOG, §§28 párr. 2, 31 párr. 2 POG RP, §34a párr. 2, 3 SOG MV, §28b párr. 4 SpolG y §34a párr. 2 ThürPAG; véase Wolter (2010: 301); sobre el servicio secreto: §§ 20n y 4a BKAG.

12. §110a Párr. 1 S. 1.StPO.

13. §98 a StPO.

14. §81a Párr. 1 StPO. Véase Welp (2002: 538).

15. BverfGE 103, 21, 34; Welp (2002: 539). La referencia a los «delitos de significativa relevancia» previstos en la ley fue considerado por el BGH en 1996 conforme a derecho («Hörfallenentscheidung«). Cf. Rieß (2004: 624).

16. Esos requerimientos son suficientes para, por ejemplo, un robo con armas, una estafa o defraudación.

El legislador ha renunciado sólo en algunos casos a la fórmula cuando ya existe un catálogo expreso de delitos (Rieß, 2004: 623), y limita habitualmente la fórmula con el requerimiento de especial relevancia del bien jurídico, o el especial interés público en la persecución penal (Paeffgen, 2001: 1.304). La nueva categoría también coincide, en algunos casos, con otras categorías ya existentes, como la de «delitos especialmente graves».[17]

Relación con otras medidas

Tal como estaba previsto en el anterior §100i párr. 1 núm. 1 StPO versión anterior, el empleo del IMSI-Catcher debería guardar una estricta relación con las medidas procesales que posteriormente se deben ordenar, como lo prevé el §160 párr. 1 StPO, como la recolección de los datos de tráfico, según el §100g StPO (Harnisch y Pohlman, 2009: 207), la detención provisional del §127 párr. 2 StPO, o del §114 StPO, o internamiento según el §126a StPO. La nueva versión del §100i StPO no prescribe nada sobre la relación causal entre el empleo del dispositivo y las medidas de investigación a las que debería dar lugar, con lo que parece constituir al IMSI-Catcher como medio de prueba autónomo, mientras que anteriormente era regulado como una precondición para asegurar medidas más intrusivas de injerencia (Wolter, 2010: 301).

Personas destinatarias de la medida

Las personas destinatarias de las medidas se encuentran mencionadas en el §100i párrafo 3 oración 1 en relación con el §100a párrafo 3 StPO, es decir, el acusado de ser autor o partícipe de un delito de significativa importancia, así como las personas acusadas de haber participado en ese delito, mediante la comisión de otro delito independiente. También se encuentran comprendidas las «personas de contacto», que son aquellas personas de las cuales se puede presumir que están en relación con el inculpado, ya sea porque envían, reciben o redireccionan mensajes destinados o relacionados con el inculpado (Hellmann, 2006: 129).[18]

La versión anterior vigente hasta el 31 de diciembre de 2007 del §100i StPO solo contemplaba al inculpado y, en forma subsidiaria, a los fines de la identificación del inculpado, a las personas de contacto. También prescribía que los números IMSI/IMEI solo podían ser captados con ayuda del IMSI-Catcher cuando no existía otro medio disponible de vigilancia menos intrusivo, y cuando la investigación del sitio en

17. Por ejemplo: § 100c I Nr. 1 StPO.

18. Sin embargo, del empleo del IMSI-Catcher puede resultar afectado un número de hasta mil o más usuarios simultáneamente. Al respecto, véase Bode (2012: 412). Aunque la afectación no resulta, para el BverfG, relevante, ver: BVerfG 2 BvR 1345/03 - 22. August 2006 (-) [= HRRS 2006 Nr. 807], núm. marg. 82; también, entre otros, Hartmann y Schmidt (2016: 214-215).

el que se encontraba el autor sería muy dificultosa por otros medios, o casi imposible (Harnisch y Pohlman, 2009: 208) (cláusula de subsidiariedad). Debido a que la nueva versión del §100i StPO no contiene ninguna cláusula de subsidiariedad respecto de otras medidas, el ámbito de aplicación del §100i StPO se expandió considerablemente. Subsiste, sin embargo, un deber de identificación de las posibles personas de contacto que deriva del derecho a negarse a prestar declaración y del secreto profesional (§101 párrafo 3 oración 1 número 8 StPO), así como de los deberes de recolección de prueba y prohibición de aplicación de la prueba (§160a párrafo 1 oración 1 hasta 4, párrafo 2 StPO).

Extensión temporal

El empleo del IMSI-Catcher requiere de una orden judicial escrita, previa a solicitud de la Fiscalía, y puede extenderse hasta seis meses (§100i párrafo 3 oración 1 en relación con el §100b párrafo 2, oración 1 StPO), aunque puede prorrogarse si subsisten los presupuestos de la medida por hasta seis meses más (§100i párrafo 3, oración 3 StPO). En caso de peligro en la demora, la Fiscalía puede ordenar su utilización, aunque la medida debe ser confirmada judicialmente dentro de los tres días posteriores (§100a párrafo 3 oración 1 en relación con el §100b párrafo 1 oración 1 hasta 3 StPO). Se debe comunicar al afectado de la conclusión de la medida (§101 párrafo, 3 oración 1, número 8 StPO).

Empleo de datos y datos relacionados con terceros

Por otra parte, los datos recolectados deben ser utilizados para la averiguación del hecho y el lugar en el que se encuentra el inculpado (§100i párrafo 1 StPO), y si bien se pueden utilizar en otros procesos, se deben reunir los presupuestos del §477 párrafo 2, oración 2 StPO (utilización de los datos por la policía ante riesgos relevantes a la seguridad pública). Aunque no sea la función primordial del dispositivo, es posible configurar un perfil de movimiento de la persona (Hilger, 2002: 557). Luego de vencido el plazo de la medida, los datos deben eliminarse cuando no son más necesarios para los fines de la persecución penal (§101 párrafo 8 StPO).

Los descubrimientos casuales sobre hechos de terceros que no son objeto de las medidas no pueden ser utilizados en procesos en su contra carecen de aplicación, por ende, las disposiciones del §477 párrafo 2, oración 2 y 3 StPO (comparar con el §477 párrafo 2, oración 4 StPO); lo mismo sucede si los datos se refieren a las personas que están autorizadas a negarse a prestar declaración testimonial, o a las que están amparadas por el secreto profesional. Luego de la finalización de la medida se deben suprimir los datos (§100i párrafo 2, oración 2 StPO), lo que debe hacerse bajo control de la Fiscalía, y posterior protocolización (§101 párrafo 8, oración 2). Los datos solo

pueden utilizarse en forma preventiva frente a peligros de la seguridad pública (§100a StPO), pero no frente a peligros para el orden público (Bruns, 2013: 530).

Examen crítico

La nueva versión del §100i StPO es mucho más amplia que la versión anterior vigente hasta 2007, pues se amplió el círculo de destinatarios, así como el catálogo de delitos a investigar; también se constituyó al empleo del IMSI-Catcher en un medio de prueba independiente (Wolter, 2010: 301), y se habilitó la posibilidad de investigar la localización del inculpado con empleo del IMSI-Catcher, al margen de que la función localizadora del dispositivo ha ido decreciendo en importancia, ante el avance tecnológico, como, por ejemplo, ante el empleo de otros medios técnicos (Harnisch y Pohlman, 2009: 210).[19]

Afectación de los derechos fundamentales

El empleo del IMSI-Catcher se debe examinar en el contexto de la vigencia de la garantía constitucional que protege el secreto de las comunicaciones (artículo 10 II GG, Ley Fundamental Alemana), y la que protege el derecho a la autodeterminación informativa (artículo 2, párrafo 1 en relación con el artículo 1, párrafo 1 GG).[20] La re-

19. El SMS silencioso se trata de una señal (denominada «ping») emitida por el ordenador o por un teléfono móvil a un número telefónico móvil, de manera que se puede lograr datos de conexión. Al crearse los datos de conexión se puede determinar el número de llamada, así como también la información sobre la celda móvil de onda en la que se encuentra el dispositivo en el momento. El poseedor del dispositivo móvil que recibe el mensaje no tiene conocimiento de su recepción. No cae dentro de la clasificación de vigilancia de la comunicación el simple envío del ping, pues con éste solo se procura la producción de datos, y no la vigilancia de las comunicaciones. En consecuencia, no se puede aplicar la garantía que protege el secreto de las telecomunicaciones, regulada por los §§100a/b StPO, pues no existe telecomunicación. A diferencia de la posición del Gobierno Federal. Tampoco es aplicable el §100i StPO, porque originariamente ha sido legislado teniendo en cuenta la aplicación del IMSI-Catcher. Además, con el IMSI-Catcher se tiene que averiguar el número IMSI/IMEI para determinar el número de teléfono, mientras que con el SMS silencioso ya se debe disponer de este dato. Cf. Eisenberg, 2005: 62-63. Tampoco corresponde aludir a las disposiciones generales en materia de prueba §§ 161, 163 StPO, pues la incorporación de medidas específicas de investigación demanda, por aplicación del principio de legalidad, la previsión de disposiciones legislativas concretas. Cf. Krüger, 2012: 609. Otra alternativa resulta del empleo de la captura de datos GPS, con fundamento en el §100h párr. 1 oración 1 núm. 2 StPO. Cf. Harnisch y Pohlman, 2009: 211.

20. En cuanto a la libertad de expresión (artículo 5 párr. 1 oración 1 GG), el empleo del IMSI-Catcher puede deshabilitar por un breve lapso las comunicaciones que operan con la antena-base, lo que podría configurar una afectación a la libertad de expresión previstas en el artículo 5 párrafo 1 oración 1 GG. La aplicación de la garantía que protege la libertad de expresión importa una afectación significativa en la libertad, cuestión que no se da en el breve lapso de interrupción del funcionamiento de la antena-base,

percusión constitucional del empleo del IMSI-Catcher ya ha sido objeto de examen por parte del BverfG en su sentencia del 22 de agosto de 2006, que motivó la reforma en vigencia a partir del 1 de enero de 2008. Las dos principales garantías constitucionales examinadas han sido la garantía que protege el secreto de las comunicaciones y el derecho a la autodeterminación informativa, como se verá a continuación.

Secreto de comunicaciones y derecho a la autodeterminación informativa

La garantía que protege el secreto de las comunicaciones es una extensión de la garantía que protege el secreto de las comunicaciones postales, y protege el tráfico a distancia, es decir, la transferencia material de información por medio de ondas sin cable, o por cable electromagnético. Se encuentran protegidos, por ende, no solo el tráfico telefónico, telefax, telegrama, ondas de radio, sino también los medios de transferencia digital, ondas móviles y tráfico de correos electrónicos por internet. Se protege tanto el contenido como la confiabilidad de la transferencia de datos, y de las circunstancias de la comunicación, lo que significa que también protege a los participantes en la comunicación, a las conexiones, así como también a los números de identificación, los intentos de comunicación y la frecuencia de comunicación (Harnisch y Pohlman, 2009: 211).

La garantía que protege el secreto de las comunicaciones se refiere también al medio de transferencia y a la confiabilidad de la comunicación. Debido a que el concepto de comunicación presupone un intercambio de información entre personas, un sector de la doctrina niega que el intercambio de información entre el dispositivo móvil y la antena esté protegido *stricto sensu* por la garantía que protege el secreto de las comunicaciones, pues no se encuentran reunidos los presupuestos del concepto de comunicación. Este mismo argumento rige para los datos transferidos, cuando el teléfono se encuentra en posición *stand by* (Harnisch y Pohlman, 2009: 211). En efecto, se ha indicado que cuando el teléfono se encuentra en función *stand by,* está disponible para la comunicación, aunque ello no significa que exista realmente una comunicación (Gercke, 2002a). A ello se ha agregado que la información sobre la localización, cuando se transmite *stand by*, informa la *potencialidad de comunicación* de alguien que se encuentra en esa posición, pero que tales datos no son una «circunstancia cercana a la comunicación»[21].

además de que el usuario cuenta con otros dispositivos para expresar su opinión. En cuanto a la libertad general de acción (artículo 2 párr. 1 GG), sí se encuentra afectado el derecho general a la libertad, que rige en forma general con respecto a las garantías más específicas. Cf. Beulke (2012: 174-175). En igual sentido, Wolter (2010: 307), con fundamento en la aplicación del ámbito de aplicación a partir de 2008.

21. Cf. Kudlich (2001: 1168); BVerfG 2 BvR 1345/03 - 22. August 2006 (-) [= HRRS 2006 Nr. 807], núm. marg. 60, aunque en tales casos se refieren a la función de localización, y no a las posibilidades de escuchar la comunicación. Este argumento se reiteró en la sentencia del BVerfG del 2 de marzo de 2010 - 1 BvR 256/08, Nr. 309 con respecto a los datos de posicionamiento, derivados de las señales *stand by* del

Por lo tanto, la garantía aplicable debería ser el derecho que protege la autodeterminación informativa.

La garantía que protege el secreto de las comunicaciones se superpone parcialmente con el derecho a la autodeterminación informativa (Harnisch y Pohlman, 2009: 212). Mientras que la primera se relaciona con la comunicación y sus circunstancias próximas, la segunda es una derivación del derecho informático fundamental[22] y procede de la jurisprudencia del BverfGE (Tribunal Constitucional Alemán) en el caso *Volkszählungsurteil* (BVerfGE 65, 1). De hecho, el derecho a la autodeterminación informativa emerge de dos fuentes: por lado, la garantía de la inviolabilidad del domicilio (artículo 13 GG) y, por el otro, la garantía que protege el secreto de las comunicaciones (artículo 10 GG), y comprende hipótesis donde se protegen datos durante el proceso de transferencia, pues se refiere a la integridad y confiabilidad del sistema de transferencia de datos empleado.[23] Este derecho garantiza a los particulares poder decidir cómo y en qué extensión se pueden captar, almacenar y utilizar datos personales en los términos de la ley de protección de datos personales.[24]

Si bien para la sentencia del 22 de agosto de 2006 del BverfG, los datos IMSI/IMEI no se relacionan con las «circunstancias próximas a la comunicación», no resultan amparados por la garantía que protege el secreto de las comunicaciones, sino por el derecho a la autodeterminación informativa.[25] No obstante, existen argumentos suficientes para ratificar la aplicación de la garantía que protege el secreto de las comunicaciones para los datos IMSI/IMEI y de posicionamiento.

Si bien podría sostenerse que el empleo del IMSI-Catcher tiene menor efecto intrusivo que la medida del §100g StPO, y afecta únicamente al derecho a la autodeterminación informativa, mientras que el §100g StPO afecta a la garantía que protege el secreto de las comunicaciones, este argumento presupone, sin embargo, que la reco-

---

teléfono móvil. Sobre esto, cf. Nachbaur (2007: 337) y Rolón (2015: 168).

22. O también: Computer-Grundrecht, cuya una traducción exacta al idioma castellano no es posible.

23. 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, núm. 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, núm. 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 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.

24. §3 párr. 1 BDSG; cf. Harnisch y Pohlman (2009: 212).

25. Cf. Nachbaur (2007: 335); también BVerfG del 2 de marzo de 2010 - 1 BvR 256/08, Nr. 309.

lección del mismo dato se puede sujetar a dos garantías diferentes, dependiendo del medio empleado: derecho a la autodeterminación informativa, cuando se hace uso del IMSI-Catcher (§100i StPO), y garantía que protege secreto de las comunicaciones, cuando se emplean otras medidas como las del §100g StPO (recolección de datos con colaboración del prestador de servicios de telecomunicaciones). Lo mismo puede decirse respecto de los datos de posicionamiento.

En contra de la posición del BverfG del 22 de agosto de 2006, Wolter ha indicado que no existe ninguna razón normativa para excluir del concepto de comunicación a los metadatos que emite el teléfono cuando éste se encuentra en posición *stand by*, y, por ende, para excluir del ámbito de vigencia de la garantía que protege el secreto de las comunicaciones a los datos transmitidos cuando el teléfono se encuentra en *stand by* (Wolter, 2010: 305).

Sin embargo, existen disposiciones que constituyen, sin duda alguna, razones normativas que hablan *a favor* de la inclusión de los datos IMSI e IMEI y los datos GPS en el ámbito de la garantía que protege el secreto de las comunicaciones, con lo que se puede arribar al mismo resultado que Wolter, pero por otro camino. De hecho, la argumentación referida a la ambigüedad del ámbito de aplicación de las garantías a los datos IMSI/IMEI y a los datos de posicionamiento pasa por alto la ampliación del catálogo de datos a recolectar autorizada por el nuevo §100g StPO y ratificada por la sentencia del BVerfG del 10 de marzo de 2010, que remite a los §§96 y 113b de la Ley de Telecomunicaciones (TKG),[26] e incorpora a los datos a ser recolectados como datos que integran la categoría «circunstancias próximas a la comunicación» a los datos IMSI e IMEI y a los datos GPS,[27] que, por lo tanto, devienen amparados por la garantía que protege el secreto de las comunicaciones.[28]

Esta última interpretación permite coordinar la relación entre el §100i con el §100g StPO, y ratificar que el empleo del §100i StPO puede servir para la realización de otras medidas de prueba.[29]

Finalmente, no hay dudas de que si se emplea el IMSI-Catcher para escuchar las

26. Boletín Oficial Alemán: BGBl. I p. 272. Nachbaur, (2007), p. 335, también BVerfG del 2 de marzo de 2010 - 1 BvR 256/08, núm. 309.

27. Sobre esta cuestión, cf. Rolón (2015: 168).

28. Cf. Roxin y Schünemann (2014: 297), núm. márg. 38 con cita de la sentencia BverfG NJW 2007, 351. De hecho, ésta era la posición del Parlamento Alemán al formular recomendaciones en 2002 al proyecto oficial. Véase Bundesrat-Empfehlung zum Entwurf der Bundesregierung (Gesetz zur Änderung der Strafprozessordnung) del 10 de junio de 2022, Drucksache 452/1/02, p. 4: La propuesta se refería al artículo 1a del Proyecto de Reformas del Gobierno Federal y decía: «Artículo 1a. Limitaciones a los derechos fundamentales: «El secreto postal y de las comunicaciones (artículo 10 de la Ley Fundamental) se limita según los términos de esta ley». El fundamento se refería a la incorporación del §100i sobre IMSI-Catcher al Código Procesal Penal Alemán (StPO).

29. Así, por ejemplo, Hartman y Schmidt (2016: 312), núm. marg. 655.

comunicaciones, la norma aplicable en tal caso son los §§100a/b StPO, y, por lo tanto, la garantía que protege el secreto de las comunicaciones (Mayer, Goßner y Schmitt, 2015: 431).

Principios constitucionales aplicables

Principio de reserva legal

El §100i StPO cumple con el mandato de reserva legal (artículo 2, párrafo 1 GG) solo desde el punto de vista formal, al regular las formas de injerencia sobre las garantías constitucionales mencionadas (Harnisch y Pohlman, 2009: 214). Desde el punto de vista sustancial, en lo que respecta al mandato de determinación como derivado del principio de reserva de la ley, el catálogo de delitos de significativa relevancia al que alude el legislador como supuesto límite del §100i StPO mediante un intento de concretización por vía del catálogo de delitos previstos en el §100a párr. 2 StPO, carece de función delimitadora, lo mismo que la exigencia de que en concreto el delito sea de significativa relevancia, sobre todo si se advierte que, de hecho, la lista a la que remite el §100i StPO no es taxativa.

Subsidiariedad y principio de proporcionalidad

Finalmente, para que el empleo del IMSI-Catcher cumpla con los requisitos del principio de proporcionalidad –derivado del estado de derecho–, es necesario que la regla legal comprenda de los tres mandatos parciales, en relación a la finalidad legítima, la adecuación y la necesidad de medidas estatales.[30]

En cuanto a la finalidad legítima del dispositivo, ésta deviene justificada por los fines de la investigación penal, y porque la averiguación de los datos IMSI/IMEI permite ordenar otras medidas de investigación (Harnisch y Pohlman, 2009: 216).

Subsisten dudas en algún sector de la doctrina en la medida en que la nueva versión del §100i StPO autoriza el empleo cumulativo del §100i junto con otras medidas, como el §100g StPO,[31] en lugar de establecer una relación subsidiaria entre ellas, con lo que el §100i StPO y el §100g StPO concurren parcialmente. La única diferencia parece ser que el §100g StPO presupone la intervención de un prestador de servicios, mientras que el §100i StPO simplemente requiere de disponer del IMSI-Catcher (Wolter, 2010: 302).

Si bien el §100i StPO carece de cláusula de subsidiariedad con respecto a otras medidas, la norma está limitada por el principio de proporcionalidad. Este límite, sin

30. Cf. Harnisch y Pohlman (2009: 215), nota 189: con otras referencias a sentencias del BVerfG.

31. Cf. Wolter (2010: 301), argumento de la preposición «además» del §100i StPO; Meyer, Goßner y Schmitt (2015: 431).

embargo, es dudoso si se advierte que la limitación del §100i StPO derivada de la aplicación del principio de proporcionalidad podría llegar demasiado tarde, ya que puede ser visto como un argumento en contra de la constitucionalidad del §100i StPO (brevemente: falta de proporcionalidad del §100i StPO).

En todo caso, el argumento no es contundente, sin examinar en *concreto* la repercusión del empleo del IMSI-Catcher según el §100i StPO. El examen en concreto de la proporcionalidad de la medida surge de la fórmula «delito de significativa importancia», y de la referencia al examen en concreto contenido en el mismo §100i StPO, que conlleva a una ponderación de la intensidad de la medida de acuerdo con cada caso (Welp, 2002: 540; Klesczewski, 2008; 28). Desde la doctrina se ha criticado esta remisión, ateniendo a la amplitud de la formula mencionada, y se ha sostenido que, en la práctica, la fórmula que concretiza el examen de proporcionalidad de la medida carece de función delimitadora real (Rieß, 2004: 623). La medida, además, afecta en concreto a un número significativo de usuarios (Roxin y Shünemann, 2014: 297), y puede afectar a las relaciones entre defensores y sus clientes.[32]

Por otra parte, en lo que respecta a la extensión temporal de la medida de seis meses (§100i párrafo 3 oración 1 en relación con el §100b párrafo 2, oración 1 StPO), se ha criticado la excesiva extensión del plazo, si se advierten que otras medidas tienen una vigencia más restringida (Wolter, 2010: 311), como, por ejemplo, §100g StPO, cuyo plazo para recolectar los datos de posicionamiento solo es de cuatro semanas.

En lo que respecta a la necesidad de su empleo, se debe usar el IMSI-Catcher sólo cuando no existen otros medios alternativos menos lesivos, por ejemplo, testigos, medidas de observación, o consulta a los prestadores de servicios en los términos de los §§112 y 113 de la Ley de Telecomunicaciones, además de que únicamente resulta aplicable a prestadores de servicios registrados en Alemania, pero no a los que se encuentran en el exterior, a quienes debe requerírsele colaboración por mecanismos internacionales de cooperación; ello, al margen de las posibilidades de comercio privado con el dispositivo.[33]

El empleo del IMSI-Catcher puede ser excluido, o acompañado por otras medidas, como, por ejemplo, cuando se aplican sobre ámbitos protegidos por otras garantías constitucionales, como la inviolabilidad del domicilio. De manera que la medida no se puede aplicar al domicilio, a espacios laborales, u oficinas de acceso no público, espacios de asociaciones, habitaciones de hotel, jardines domiciliarios, etcétera (Gercke, 2002: 127).

32. Argumento del apelante en la sentencia BVerfG 2 BvR 1345/03 - 22. August 2006 (-) [= HRRS 2006 núm. 807], núm. márg. 25.

33. Argumento del apelante en la sentencia BVerfG 2 BvR 1345/03 - 22. August 2006 (-) [= HRRS 2006 Nr. 807], núm. marg. 24.

Con presupuestos similares a los anteriormente mencionados —es decir, delito de significativa relevancia, en abstracto y en concreto, una cláusula de subsidiariedad que se refiere al principio de proporcionalidad y un catálogo de delitos limitado por el §100c II StPO—, el IMSI-Catcher contempla además la vigilancia acústica del domicilio (§§100c StPO y siguientes «*großer Lauschangriff*», «gran escucha»), con el fin de averiguar el lugar donde se encuentra el inculpado, o la averiguación de la verdad. Sin embargo, esta medida no se relaciona con las comunicaciones como lo hacen las hipótesis de los §§100a, 100b StPO, y, por ende, no se relaciona con la vigilancia de las telecomunicaciones (Bratke, 2013: 58).

La vigilancia acústica de espacios que no están protegidos por la garantía de inviolabilidad del domicilio está regulada en el §100f StPO («kleiner Lauschangriff», «pequeña escucha») (Bratke, 2013: 69). Además, en forma alternativa o complementaria, y a los fines del examen de la proporcionalidad de la medida, no solo se puede ordenar la observación (§100h StPO: 163 y ss. StPO), sino también el empleo de personas de identidad reservada o de confianza o investigadores encubiertos (§§100a y ss. StPO) y medidas ordinarias de investigaciones (§§102 y ss. StPO).

Asimismo, para la determinación del lugar donde se encuentra la persona sospechosa o inculpada, se puede intentar determinar su posición con ayuda de datos GPS —en tal caso recurriendo a la medida del §100g StPO—, o bien con empleo del SMS silencioso, cuya ventaja radica en ser más rápido y eficiente. Este último caso, sin embargo, si bien es más efectivo, es dudoso que se encuentre previsto legalmente,[34] y una remisión a la cláusula general probatoria para la investigación prevista en el §163 StPO[35] se presenta desde el punto de vista metodológico, como una invitación a la psicología de las libres asociaciones, bajo pretexto de la analogía, o de la libertad probatoria, o bajo el pretexto de excepciones a derivaciones de otras garantías como el *nemo tenetur*, y, devienen, por ende, imposibles de refutar, por lo que deben descartarse, a falta de disposición expresa, que realice el principio de reserva legal. Finalmente, con respecto a la adecuación (proporcionalidad en sentido estricto) se debe evaluar la repercusión de la medida sobre terceros no inculpados (Harnisch y Pohlman, 2009: 216), por lo tanto, la medida debe ser ordenada en la medida en que

34. Cf. Harnisch y Pohlman (2009: 216); en tal caso debe hacerse con fundamento en el §100a StPO o de la cláusula general de prueba del §161 StPO, pero no en el §100i StPO que únicamente se refiere al IMSI-Catcher; véase Mayer, Goßner y Schmitt (2015: 431), núm. marg. 4.

35. Sólo traduciré a la parte pertinente a los fines de este comentario del §163 StPO, en este caso, sólo el primer párrafo: «Los funcionarios y oficiales del servicio policial deben investigar los delitos, y deben disponer sin demora de las medidas para aclarar el hecho. A tales fines están autorizados a obtener informes de todas las autoridades, y a exigir información en caso de peligro de demora, así como también a emprender investigaciones de todo tipo, siempre que otras reglas no regulen sus poderes en forma específica». La disposición relativa a la actuación de la fiscalía contenida en el §161 StPO tiene un tenor prácticamente idéntico, sólo que se refiere a la fiscalía.

intereses de mayor relevancia tengan prioridad por sobre los derechos de los afectados, lo cual resulta dudoso si se advierte que tales factores son difíciles de determinar mediante una ponderación *ex ante*.

Conclusiones

Se tiene que distinguir el IMSI-Catcher como dispositivo, y la regulación de su empleo en el §100i StPO. El IMSI-Catcher puede tener diferentes funciones. Tales funciones deben ser interpretadas de acuerdo con el plexo normativo relativo a la prueba en el proceso penal. Así, por ejemplo, si se utiliza el IMSI-Catcher para escuchar conversaciones, la normativa aplicable es el §100a/b StPO. Si el IMSI-Catcher se utiliza para recolectar datos IMEI/IMSI, el §100i StPO tiene una función específica respecto del §100g StPO, que requiere colaboración del sector privado.

Si, por otra parte, el IMSI-Catcher se utiliza para confeccionar un perfil de movimiento, se debería tratar de una hipótesis análoga a la vigilancia acústica fuera del domicilio, regulada en el §100f StPO, aunque más específica, al estar regulada especialmente en el §100i StPO; o bien debería ser tratada como un caso más específico que el previsto en el §163 StPO sobre medidas de observación, y, por ende, más coherente con el principio de reserva de la ley procesal penal. Sin embargo, el carácter tan específico del §100i StPO, al estar centrado en el medio técnico, y no en la función, es un argumento *contra* la incorporación de innovaciones técnicas, con menores efectos colaterales y mayor eficacia, como puede evidenciarlo el empleo el SMS silencioso, si se acepta que la utilización del *stealth SMS* carece de anclaje legal. Una vigilancia dentro del domicilio, como la que habilita la vigilancia acústica del §100c StPO, sería ineficaz, pues el uso del dispositivo no requiere ingresar en la esfera de privacidad e intimidad de la persona.

La incorporación de los datos IMSI/IMEI y de los datos de posicionamiento al catálogo de datos que pueden ser objeto de recolección en el §100g StPO, implica que los datos IMSI/IMEI (eventualmente denominados «metadatos») forman parte de la definición de comunicaciones, según la Ley de Telecomunicaciones, y, por lo tanto, su captura debería ser comprendida por la garantía que protege el secreto de las comunicaciones. De lo contrario, no se explicaría la razón por la cual el mismo dato está protegido por la garantía que protege el secreto de las comunicaciones, si es recolectado con fundamento en el §100g StPO, y por el derecho a la autodeterminación informativa, si es recolectado mediante el IMSI-Catcher, según lo prescripto en el §100i StPO.

Referencias

Beulke, Werner (2012). *Strafprozessrecht*. 12.ª ed. Heidelberg: C. F. Muller.

Bode, Thomas A (2012). *Verdeckte strafprozessuale Ermittlungsmaßnahmen*. Berlin/Heidelberg: Springer.

Bratke, Bastian (2013). *Die Quellen-Telekommunikationsüberwachung im Strafverfahren. Grundlagen, Dogmatik, Lösungsmodelle*. Berlin: Duncker & Humblot.

Bruns, Michael (2013). Comentario al §100i StPO, en Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK, edición a cargo de Hannich, Rolf. Berlin: C. H. Beck.

Eisenberg, Ulrich y Tobias Singelnstein (2005). «Zur Unsulässigkeit der heimlichen Ortung per 'stiller SMS.». *Neue Zeitschrift für Strafrecht*. Berlin/Frankfurt: C. H. Beck.

Eschelbach, Ralf (2014). Comentario al §100i StPO., en StPO Strafprozessordnung. Mit GVG und EMRK Kommentar, edición a cargo de Satzger, Helmut, Wilhelm Schluckebier y Gunter Wildmaier. Colonia: Carl Heymanns.

Gercke, Björn (2002a). *Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren. Zugleich ein Beitrag zur Kumulation heimlicher Observationsmittel im strafrechtlichen Ermittlungsverfahren*. Berlin: Duncker & Humblot.

—. (2002b). «Überwachung der Mobilfunkverkehrs –das Handy als 'Aroundmittel' zur Ausforschung». CILIP, 071: P. Disponible en http://bit.ly/20YtjZy.

Harnisch, Stefanie y Martin Pohlman (2009). «Strafprozessuale Maßnahmen bei Mobilfunkendgeräten. Die Befugnis zum Einsatz des sog. IMSI-Catchers». *Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht*, 10: 202-220. Disponible en http://bit.ly/2ksF9GI.

Hartmann, Arthur y Rolf Schmidt (2016). *Strafprozessrecht: Grundzüge der Strafverfahrens*. 6.ª ed. Rolf Schmidt.

Hellmann, Uwe (2006). *Strafprozessrecht*. 2.ª ed. Berlin: Springer.

Hilger, Hans (2002). «Gesetzgebungsbericht: Über en neuen §100i StPO». *Goldtammers Archiv für Strafrecht*.

Klesczewski, Diethelm (2008). «Kritik der Vorratsdatenspeicherung», en *Festschrift für Gerhard Fezer zum 70.* Geburtstag am 29. Oktober 2008, edición a cargo de Weßlau, Edda y Wohlers Wolfgang. Berlin/Nueva York: De Gruyter.

Krüger, Christine (2012). «Die sogenannte 'stille SMS' im strafprozessualen Ermittlungsverfahren. Erkenntnisse zum Einsatz in der Praxis und Betrachtung der rechtlichen Anwendungsvoraussetzungen». Zeitschrift für das Jurisdiche Studium (ZJS) 5/2012. Disponible en http://www.zjs-online.com/dat/artikel/2012_5_615.pdf.

Kudlich, Hans (2001). «Mitteilung der Bewegungsdaten eines Mobiltelefons als Überwachung der Telekommunikation - BGH, NJW 2001, 1587. *Juristiche Schulung*, 2001 Heft 12.

Mayer-Gossner, Lutz y Bertram Schmitt (2015). *Strafprozessordnung mit GVG und Nebengesetzen*. 58.ª ed. Munich: C. H. Beck.

Nachbaur, Andreas (2007). «Standortfestellung und Art. 10 GG-Der Kammerbeschluss des BverfGE zum Einsatz des 'IMSI-Catchers'». Neue Juristiche Wochenzeitschrift (NJW). Múnich/Frankfurt: C. H. Beck.

Paeffgen, Hans-Ulrich (2001). «Überlegungen zu einer Reform des Rechts der Überwachung der Telekommunikation», en *Festschrift für Claus Roxin zum. 70* Geburstag am 15. Mai 2001, edición a cargo de Achenbach, Hans, Wilfried Bottke, Bernhard Haffke, Hans-Joachim Rudolphi y Bernd Schünemann. Berlin/Nueva York: De Gruyter.

Riess, Peter (2004). «Die Straftat von erheblicher Bedetung' als Engriffsvorausetzung Versuch einer Inhaltsbestimmung». *Goldtammer's Archiv für Strafrecht*. Heidelber: R.V. Decker.

Rolón, Darío (2015). «Acceso procesal a datos alojados en el proveedor de servicios de telecomunicaciones (TSP) según la ordenanza procesal penal alemana (ref. esp §100g StPO)». *Revista de Estudios de la Justicia*, 23. Disponible en http://bit.ly/2Dg22F6.

Roxin, Claus y Bernd Schünemann (2014). *Strafverfahrensrecht*. 28.ª ed. Múnich: C. H. Beck.

Schäfer, Gerhard (2004). «Comentario al §100i StPO». En *Die Strafprozessordnung und Gerichtsverfassungsgesetz. Großkommentar*. 25a edición a cargo de Rieß, Peter. II Band §§ 72-136a. Berlín/Nueva York: De Gruyter.

Welp, Jürgen (2010). «Verbindungsdaten. Zur Reform des Auskunftrechts (§§ 100 g, 100 h StPO). *Goldtammer's Archiv für Strafrecht*. Múnich/Frankfurt: C. H. Beck.

Wolter, Jürgen (2010). Comentario al §100i StPO, en SK-StPO Systematischer Kommentar zur Strafprozessordnung. Mit GVG und EMRK, Band II §§94-36a StPO. 4.ª ed. a cargo de Jürgen Wolter. Colonia: Carl Heymanns.

Sobre el autor

Darío Nicolás Rolón es LL.M Goethe Universität Frankfurt am Main. Doctorando en la Friedrich Alexander Universität Erlangen-Nürnberg. Ex Becario del Servicio de Intercambio Alemán (DAAD) en la Lüdwig Maximilians Universität München y de la Stiftung der Hessischen Rechtsanwaltschaft. Su correo electrónico es nrolon_@hotmail.com.

REVISTA DE ESTUDIOS DE LA JUSTICIA

La *Revista de Estudios de la Justicia* es publicada, desde 2002, dos veces al año por el Centro de Estudios de la Justicia de la Facultad de Derecho de la Universidad de Chile. Su propósito es contribuir a enriquecer el debate jurídico en el plano teórico y empírico, poniendo a disposición de la comunidad científica el trabajo desarrollado tanto por los académicos de nuestra Facultad como de otras casas de estudio nacionales y extranjeras.

DIRECTOR

Álvaro Castro
(acastro@derecho.uchile.cl)

SITIO WEB

rej.uchile.cl

CORREO ELECTRÓNICO

cej@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.cl).