Boletín de Jurisprudencia
Septiembre 2024

EVIDENCIA DIGITAL Y DERECHOS HUMANOS:
Desafíos jurídicos en la era tecnológica

ESCUELA DE LA DEFENSA PÚBLICA
MPD Argentina
30 AÑOS DE AUTONOMÍA
O.D.I.A. OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO

ÍNDICE

Escuela de la Defensa Pública de la Defensoría General De La Nación

El Ministerio Público de la Defensa de la Nación es una institución del sistema de justicia nacional y federal que se encarga de la defensa y protección de los derechos humanos. El MPD garantiza el acceso a la justicia y la asistencia jurídica integral, en casos individuales y colectivos, en especial de quienes se encuentren en situación de vulnerabilidad. La Constitución Nacional, en su artículo 120, instituye el MPD como un órgano independiente del resto de los poderes del Estado, con autonomía funcional y autarquía financiera. La Escuela de la Defensa Pública es responsable de las actividades de formación, actualización y perfeccionamiento que se realizan en el Ministerio Público de la Defensa. Su proyecto pedagógico se apoya en el empleo de diferentes estrategias; entre ellas, gestiona un ecosistema profesional en el que promueve la circulación y la producción de información jurídica con perspectiva de derechos humanos. En ese marco, el presente repositorio pone a disposición de toda la comunidad la selección y recopilación de jurisprudencia y otros materiales jurídicos producidos por el Ministerio Público de la Defensa.

Observatorio de Derecho Informático Argentino (O.D.I.A.)

El Observatorio de Derecho Informático Argentino (O.D.I.A.) es una asociación civil sin fines de lucro. Fue creada con el objetivo de promover el ejercicio responsable de la ciudadanía digital y garantizar que los derechos de la comunidad sean respetados. O.D.I.A. lleva adelante trabajos de investigación, difusión, capacitaciones y litigio estratégico. Cuenta con profesionales del mundo del derecho y de la informática, y también personas provenientes de diferentes ámbitos interesadas en el cruce del derecho y de las tecnologías de la información. La interdisciplinariedad es un eje central al momento de investigar con rigurosidad técnica aquellas situaciones derivadas del uso de nuevas tecnologías y cómo afectan la vida cotidiana de las personas.

INTRODUCCIÓN

Escuela De La Defensa Pública
Defensoría General De La Nación

El boletín "Evidencia digital y derechos humanos: Desafíos jurídicos en la era tecnológica" fue elaborado por la Escuela de la Defensa Pública de la Defensoría General de la Nación y es el segundo documento del Dossier "Nuevas tecnologías y derecho". Para la sistematización del documento y para la identificación de casos relevantes, contamos nuevamente con la colaboración de Antonella Bentín, Secretaria de Primera Instancia de la Defensoría Pública Oficial Federal de Concordia, provincia de Entre Ríos.

Este documento recopila jurisprudencia nacional e internacional sobre la evidencia digital y su impacto en los derechos fundamentales. Se examinaron 26 sentencias de diversos tribunales, nacionales e internacionales, emitidas entre 1999 y 2023, que hicieron lugar al planteo de la defensa. Respecto a la distribución de la jurisprudencia analizada, 9 corresponden a decisiones dictadas por tribunales de Argentina, 6 a Estados Unidos y 1 a Alemania; otras 9 son decisiones dictadas por el Tribunal Europeo de Derechos Humanos y 1 por la Corte Interamericana de Derechos Humanos.

La diversidad de fuentes permite una visión comparada de cómo las diferentes jurisdicciones abordan algunos de los desafíos que presenta la evidencia digital en el ámbito judicial. Además, la jurisprudencia analizada revela las tensiones que surgen cuando se pretende obtener y utilizar esta evidencia y se cuenta con un marco legal que en muchos casos no la prevé expresamente y que ha sido diseñado para regular otro tipo de pruebas.

Las sentencias fueron sistematizadas y agrupadas en ocho áreas temáticas: desbloqueo compulsivo de dispositivos electrónicos; geolocalización, vigilancia electrónica e interceptación de comunicaciones; alcance de registros y hallazgos incidentales en evidencia digital; monitoreo e interceptaciones electrónicas y registro remoto de sistemas; límites en la búsqueda de información en pericias informáticas y protección de datos personales; prueba digital obtenida a través de medios ilícitos; protección de datos personales y libertad de expresión en el ámbito digital; y prueba informática y cadena de custodia.

La estructura de categorías separadas en este boletín responde a la complejidad y diversidad del campo de la evidencia digital y los derechos humanos.

En el ámbito del desbloqueo compulsivo de dispositivos electrónicos (acápite 1), se analizan dos casos de jurisprudencia internacional que abordan el delicado equilibrio entre la necesidad de investigación criminal y el derecho fundamental a no autoincriminarse. En esas decisiones se discutieron los límites constitucionales del acceso a dispositivos electrónicos en el contexto de investigaciones, considerando aspectos como el uso de características biométricas y las implicancias del desbloqueo forzoso en términos de autoincriminación.

Bajo el título “Geolocalización, vigilancia e interceptación de comunicaciones” (acápite 2) se presentan siete casos de jurisprudencia internacional en los que se debatió sobre el acceso a datos de localización y la implementación de sistemas de vigilancia masiva. Los pronunciamientos abordan cuestiones como la necesidad de órdenes judiciales para acceder a registros de localización de teléfonos móviles, los requisitos para la legalidad de la geolocalización en tiempo real y las garantías necesarias en las leyes que regulan la vigilancia secreta.

En cuanto al alcance de registros y hallazgos incidentales en evidencia digital (acápite 3), se analizan tres casos, uno de jurisprudencia nacional y dos de jurisprudencia internacional, que

discuten pautas sobre cómo adaptar los principios tradicionales de búsqueda e incautación al contexto digital. Estas decisiones abordan temas como la necesidad de protocolos de búsquedas específicos y los límites de la doctrina de la "*plain view*" en el ámbito digital.

En el acápite 4 "Monitoreo e interceptaciones electrónicas. Registro remoto de sistemas informáticos", se presenta un caso de jurisprudencia internacional que establece un nuevo derecho fundamental a la protección de la confidencialidad e integridad de los sistemas de información. Esta decisión es importante para comprender las implicancias legales de las prácticas de infiltración y monitoreo de sistemas informáticos completos.

En el área de límites en la búsqueda de información en pericias informáticas y protección de datos personales (acápite 5), se agruparon siete fallos, tres de jurisprudencia nacional y cuatro de jurisprudencia internacional, que permiten reflexionar sobre los límites de la recopilación y retención de datos personales en investigaciones criminales. Estos casos abordan temas como los estándares de protección de datos en investigaciones penales y la retención de datos biométricos.

En el acápite 6 "Prueba digital obtenida a través de medios ilícitos" se agruparon dos decisiones de jurisprudencia nacional que abordan la exclusión de prueba digital por haber sido obtenida de forma ilegal.

En cuanto a la protección de datos personales y libertad de expresión en el ámbito digital (acápite 7), se examinan tres casos, dos de jurisprudencia nacional y uno de jurisprudencia internacional, que abordan la compleja interacción entre estos derechos fundamentales. Los casos analizados tratan temas como la violación de secretos, el uso indebido de información confidencial y los límites de la libertad de expresión en el contexto de investigaciones penales en el entorno digital. Adicionalmente, se explora el concepto de autodeterminación informativa como componente esencial del derecho a la privacidad, estableciendo un vínculo crucial entre la protección de datos personales y el ejercicio de la libertad de expresión. La jurisprudencia también enfatiza la obligación estatal de garantizar que la recopilación, uso y tratamiento de datos personales se realice de manera legal y respetuosa con los derechos humanos, particularmente en contextos sensibles como el de los defensores de derechos humanos.

Finalmente, en el ámbito de prueba informática y cadena de custodia (acápite 8), se resume un pronunciamiento de jurisprudencia nacional en el que se discuten los requisitos técnicos y legales que garantizan la validez de las pericias informáticas en procesos judiciales. Este caso aborda la necesidad de notificar a la defensa de la realización del peritaje y la importancia de mantener la integridad de la evidencia digital a lo largo de todo el proceso judicial.

Es importante señalar que la jurisprudencia en este campo está en constante evolución, reflejando los rápidos avances tecnológicos y los nuevos desafíos que estos plantean para el derecho. Por ello, este boletín debe considerarse como un punto de partida para el análisis de estos temas, más que como un compendio definitivo.

Invitamos a los lectores a contribuir a la expansión y actualización de este recurso. Si conocen pronunciamientos relevantes no incluidos en este boletín, les pedimos que nos escriban a jurisprudencia@mpd.gov.ar. Su aporte será fundamental para mantener este recurso actualizado y completo, asegurando su utilidad para profesionales del derecho, académicos y todos aquellos interesados en la intersección entre tecnología y derechos fundamentales.

PRESENTACIÓN

Observatorio de Derecho Informático Argentino (O.D.I.A.)

Bajo el tópico "evidencia digital" el Boletín presenta una serie de problemas —algunos novedosos— en torno a: el uso de dispositivos tecnológicos para la investigación criminal; el secuestro y análisis de dispositivos en poder de personas sospechadas de la comisión de delitos; la exigencia de contar con una legislación precisa y adecuada que reglamente su empleo con anterioridad al hecho investigado; y la afectación de derechos y garantías de orden constitucional y convencional —principalmente el derecho a la intimidad— que su uso provoca cuando no existe una legislación adecuada o control judicial.

No es una compilación exhaustiva y sistemática pero su acierto reside en seleccionar una serie de fallos de los últimos veinte años, de distintas latitudes, instancias y ordenamientos jurídicos, que guardan relaciones entre sí: seis fallos norteamericanos; uno del Tribunal Constitucional Alemán, uno de la Corte Interamericana de Derechos Humanos y nueve del Tribunal Europeo de Derechos Humanos; y, para cerrar, una serie de fallos locales, de las jurisdicciones Federal, Nacional y de la Ciudad Autónoma de Buenos Aires.

Para que el lector pueda orientar su lectura en razón de sus necesidades, aprovecharemos esta introducción para reseñar brevemente el tema sobresaliente de los casos elegidos.

Comencemos con la jurisprudencia estadounidense, enfocada en la extensión de la protección contra la autoincriminación. En el primer caso, N° 4-19-70053, el Tribunal del Distrito Norte de California resolvió si el uso de características biométricas de un sospechoso para desbloquear un dispositivo tecnológico estaba comprendido dentro de una expresión "testimonial" en virtud de la Quinta Enmienda que protege contra la autoincriminación. Para ello, sostuvieron que el caso no podía ser comparado con proporcionar una muestra de sangre o cabellos o proporcionar un ejemplar de escritura o voz —que no están amparados por la garantía— y luego reseñaron los precedentes que sostuvieron que no se puede obligar a una persona a aportar el código numérico o alfanumérico para desbloquear un dispositivo en virtud de la Quinta Enmienda, porque el acto de comunicar el código de acceso es testimonial, ya que "la expresión del contenido de la mente de una persona entra de lleno en la protección de la Quinta Enmienda".

En el segundo caso, "Katelin Eunjoo Seo v. Estado de Indiana", la Corte Suprema del Estado de Indiana abordó la cuestión de si forzar a una persona a desbloquear su teléfono inteligente violaba su derecho a no autoincriminarse, también protegido por la Quinta Enmienda. La Corte examinó la naturaleza única de los teléfonos inteligentes modernos, que tienen la capacidad de almacenar grandes volúmenes de información personal, y sostuvo que obligar a desbloquear un teléfono no podía compararse con la simple entrega de documentos específicos, como se había interpretado en la "excepción de conclusión previsible". Finalmente, concluyó que forzar el desbloqueo de un teléfono inteligente es un acto testimonial protegido por la Quinta Enmienda, ya que implica "la revelación del contenido de la mente" de la persona involucrada.

En los tres casos siguientes, el estándar de análisis es la "expectativa razonable de privacidad" —con los desarrollos posteriores al precedente "Katz"—; esa es la vara que utilizan los tribunales para evaluar y resolver los conflictos entre el derecho a la intimidad y las injerencias por parte del estado en el marco de investigaciones penales.

En el caso "Carpenter", la Corte Suprema de Justicia sostuvo que resultaba necesaria una orden judicial para requerir los registros de los celulares con el fin de determinar las ubicaciones de un sospechoso en un período de tiempo. El fallo es de interés porque presenta una arista distinta del

precedente “Jones”. Mientras que en “Jones” la Corte falló en torno a la colocación de un GPS en el auto de un sospechoso por parte del FBI sin autorización judicial, en este caso la Fiscalía pidió información a la empresa de telefonía móvil en base a una ley (*Stored Communications Act*). La Corte —negándose a extender los precedentes “Smith” y “Miller”, donde se sostuvo que una persona no tiene una expectativa legítima de privacidad en la información que entrega voluntariamente a terceros— sostuvo que permitirle al gobierno el acceso sin restricciones a la base de datos de los registro de las compañías de celulares contraviene la expectativa legítima de privacidad del acusado en su ubicación física.

Posteriormente, el caso “Comprehensive Drug Testing” trata sobre un secuestro amplio e irrestricto de información personal y sensible de los jugadores de baseball de la Liga Nacional, en el marco de una investigación por el uso de sustancias prohibidas.

Por último, en “Carey” se discutió la aplicación de la doctrina “*plain view*” al examinar dispositivos electrónicos. En el marco de una investigación por la presunta tenencia y comercialización de estupefacientes, por orden judicial se registró una computadora que había sido secuestrada. La orden limitó la búsqueda a archivos relacionados con la venta de estupefacientes, pero se identificaron varios archivos en formato "JPG" que, al ser abiertos, contenían fotografías con pornografía infantil. El Tribunal de Apelaciones del Décimo Distrito sostuvo que el registro que descargó las imágenes fue ilegítimo ya que ‘la doctrina de la *plain view* no puede ser utilizada para extender una búsqueda exploratoria general de un objeto a otro hasta que al final surja algo incriminatorio’, sobre todo cuando el alcance del registro se circunscribía a las pruebas relacionadas con el tráfico de drogas. Es de destacar que el Tribunal no tuvo en consideración la analogía que hizo la Fiscalía entre la computadora examinada y un “archivador” que contiene papeles al sostener: ‘Dado que es probable que el almacenamiento electrónico contenga una mayor cantidad y variedad de información que cualquier método de almacenamiento anterior, las computadoras son objetivos tentadores en la búsqueda de información incriminatoria’ [...]. Depender de analogías con contenedores cerrados o archivadores puede llevar a los tribunales a ´simplificar excesivamente un área compleja de las doctrinas de la Cuarta Enmienda e ignorar las realidades del almacenamiento masivo en computadoras modernas´, al tiempo que resaltó que se pueden emplear varios métodos para evitar buscar archivos del tipo no identificado en la orden como observar los tipos de archivos y títulos enumerados en el directorio, hacer una búsqueda de palabras clave para términos relevantes, o leer partes de cada archivo almacenado en la memoria.

En el caso del Tribunal Constitucional Federal alemán se analizó la constitucionalidad de un artículo de la Ley de Protección de la Constitución de *Nordrhein-Westfalen* que otorgaba facultades para la observación y la investigación secreta en internet y el acceso secreto a sistemas informáticos, tanto mediante programas que permitían la vigilancia a distancia como autorizando el uso de dispositivos físicos que permitían acceder a datos de manera subrepticia del sistema informático. Al fallar, la Corte reconoció “un nuevo derecho fundamental constituido por la garantía a la «confidencialidad e integridad de la información en sistemas informáticos» como una derivación del derecho a la privacidad y personalidad de los ciudadanos en el ámbito de los sistemas informáticos y comunicacionales”. El Tribunal decidió que el artículo que incluía estos medios de investigación constituía una intromisión a la intimidad y una afectación a ese nuevo derecho, razón por la cual lo declararon inconstitucional.

La Corte Interamericana de Derechos Humanos, en el caso "Miembros de la Corporación de Abogados 'José Alvear Restrepo (CAJAR) v. Colombia", reconoció el "derecho a la autodeterminación informativa" como un derecho autónomo, derivado de los artículos 11 y 13 de la Convención Americana. Para ese Tribunal, este derecho, que protege la privacidad y sirve como garantía para otros derechos, se extiende a cualquier dato personal en poder de organismos públicos y privados, otorgando a las personas la facultad de acceder, rectificar, cancelar y

oponerse al tratamiento de sus datos. La Corte enfatizó la necesidad de marcos legales claros y precisos para regular las actividades de inteligencia, especialmente en relación con periodistas y abogados, subrayando la importancia de la supervisión independiente y los recursos efectivos para proteger los derechos individuales frente a la vigilancia estatal.

Los nueve fallos del Tribunal Europeo de Derechos Humanos (TEDH) tienen en común que constituyeron violaciones al artículo 8 del Convenio que protege la vida privada y exige que cualquier injerencia al derecho deba estar prevista por una ley sancionada para cumplir con alguno de los objetivos señalados en el artículo. El caso "Ben Faiza v. Francia" trató sobre el uso de un GPS, escuchas telefónicas y captura de imágenes. En "Zoltán Varga v. Eslovaquia", el Servicio de Inteligencia Eslovaco dispuso una serie de medidas de vigilancia electrónica a un expolicía sospechado de estar implicado en actividades delictivas. En "Saber v. Noruega" una persona que se presentó como víctima de un delito entregó su teléfono a la policía y al analizarlo descubrieron comunicaciones entre el denunciante y sus abogados defensores en otro caso en el que era sospechoso de haber cometido un delito distinto. Más allá del problema en torno al derecho a la intimidad, el tribunal analizó si la ley específica y los métodos de análisis del dispositivo tecnológico respetaban el privilegio legal profesional entre cliente y abogado. Y en "Särgava v. Estonia", la policía investigó a un abogado por su presunta implicación en un delito y llevó a cabo un registro en su domicilio, su estudio y sus vehículos en los cuales secuestró y examinó su computadora personal y su teléfono móvil.

Adicionalmente, el caso "Roman Zakharov v. Rusia" se discutió la interceptación de comunicaciones móviles sin salvaguardias adecuadas contra abusos ni límites claros. El TEDH encontró que el sistema de interceptación secreto en Rusia violaba el artículo 8 del Convenio Europeo de Derechos Humanos. Para ello, señaló las deficiencias en el marco legal que regulaba las circunstancias para la vigilancia secreta y los procedimientos de autorización. Asimismo, criticó la falta de supervisión efectiva y de notificación a las personas sometidas a vigilancia. En "Big Brother Watch y otros v. el Reino Unido" se examinó el régimen de interceptación masiva, el intercambio de inteligencia y la adquisición de datos de comunicaciones. El Tribunal consideró que el régimen de interceptación masiva del Reino Unido violaba los artículos 8 y 10 del Convenio. Además, condenó la falta de supervisión adecuada sobre la selección de "selectores fuertes" y la ausencia de salvaguardias para la selección de datos de comunicaciones. Sin embargo, no se encontró violación en el régimen de intercambio de inteligencia con servicios extranjeros. En "Ekimdzhiev y otros v. Bulgaria" se analizó la vigilancia secreta y la retención de datos de comunicaciones. El Tribunal concluyó que el sistema búlgaro violaba los artículos 8 y 13 del Convenio. Al respecto, señaló la falta de claridad en la legislación sobre la autorización de vigilancia secreta y la ausencia de salvaguardias efectivas contra el abuso. Asimismo, criticó la falta de garantías suficientes contra el acceso arbitrario a los datos retenidos y la ausencia de recursos efectivos para impugnar la legalidad de las medidas de vigilancia.

El caso "Trajkovski y Chipovski v. Macedonia del Norte" trató sobre la toma y retención de muestras de ADN sin explicación o consentimiento. Mientras que "Gaughran v. el Reino Unido" se centró en la retención indefinida de datos biométricos de personas condenadas.

En todos estos casos se emplearon sistemas de vigilancia electrónica y programas y métodos de análisis de los dispositivos para la extracción de información que no estaban reglamentados por ley, o que su reglamentación era deficiente. Para el TEDH la ley que reglamenta la utilización de sistemas de vigilancia electrónica o cualquier otra tecnología que permita extraer información de carácter personal debe utilizar términos lo suficientemente claros para que cualquiera comprenda en qué circunstancias y bajo qué condiciones habilita a los poderes públicos a realizar medidas de investigación secretas y virtualmente peligrosas para el derecho al respeto de la vida privada. La legislación debe ser clara, precisa y rodeada de las garantías adecuadas contra el uso arbitrario o diversos abusos posibles.

Finalmente, los fallos locales toman muchas de las líneas jurisprudenciales antes reseñadas. En el caso "Robles" la Fiscalía desestimó una denuncia penal basada únicamente en capturas de pantalla de conversaciones de un funcionario público que podrían haber sido obtenidas mediante actividades de inteligencia ilegal, y/o publicadas o "filtradas" por medio informáticos sin consentimiento de alguno de los distintos interlocutores. En "Van Meel" también se analiza la legalidad del proceso de obtención de la prueba adquirida. La querella tomó conocimiento de una reunión entre el acusado y sus abogados, alquiló la habitación conjunta, grabó la reunión y luego aportó las desgrabaciones como prueba. El órgano revisor comenzó distinguiendo el caso con los supuestos de grabaciones sucedidas entre dos interlocutores en los que uno de ellos presenta como prueba la conversación en la que participó. Aquí, la querella no formó parte del círculo de personas que intervinieron en la reunión, lo que constituyó, en primer lugar, una intromisión en la privacidad de aquellos y en segundo, una afectación al secreto profesional y a la protección de confidencialidad de las conversaciones entre cliente y abogado. El caso "C, M" es similar al caso "Carpenter": la fiscalía, sin autorización judicial, solicitó la geolocalización del acusado a través de las conexiones de su teléfono celular. La Cámara de Apelaciones de la Ciudad, al confirmar la decisión del Juez de primera instancia que declaró nula dicha prueba remarcó que dichos procedimientos "...permiten averiguar los hábitos de un individuo, los lugares que habita, sus relaciones interpersonales, sus pasatiempos y demás cuestiones que merecen un tratamiento especial en relación con el derecho a la intimidad y la privacidad. La magnitud de la injerencia en la intimidad de personas concretas, determinadas en el caso, es inaceptable sin intervención judicial que la autorice y la controle." En "Villalba Cuyarí", la misma Cámara confirmó una resolución que autorizó el registro de un teléfono celular, en el marco de una investigación por estupefacientes, pero obligó a juez de primera instancia a que determine un período temporal preciso que delimite su alcance para no afectar el derecho a la intimidad de manera desproporcionada. En la causa N° 46.744. 24/05/2012, la Cámara Federal declaró la nulidad de los peritajes producidos por la Policía Federal y la UBA respecto de las computadoras secuestradas en un caso por enriquecimiento ilícito de un exfuncionario público. Los puntos relevantes del caso son la necesidad de garantizar la participación de la defensa en los peritajes, la necesidad de preservar correctamente la cadena de custodia de los elementos secuestrados y la complejidad técnica que tienen esos tipos de peritajes. En la causa nro. 2134/2018, la Cámara de Apelaciones de la Ciudad falló de manera similar al caso "Carey". En una investigación por amenazas realizadas por Facebook se allanó el domicilio del sospechoso y se secuestraron dos teléfonos celulares y una CPU. Al buscar prueba sobre el objeto de investigación la policía informó que se habían encontrado "imágenes con presuntos desnudos de menores que no son de interés para la presente causa". Este hallazgo fue logrado en base a la utilización de un software específico que busca imágenes referentes a posibles desnudos de menores. Se sostuvo que el peritaje fue excesivo y desproporcionado para el objeto de la investigación y que la utilización del programa *´Griffeyes Analyze´*, especializado en la búsqueda de imágenes y videos referentes a presuntos desnudos de menores, resultó una 'excursión de pesca' y una violación a la privacidad del imputado que de ningún modo estuvo justificada ni podía calificarse como un descubrimiento accidental o espontáneo.

Los fallos seleccionados brindan un panorama de los principales problemas que suscita el empleado de dispositivos de tecnología informática con fines de vigilancia y sobre los modos de obtención y producción de la prueba digital. Resulta imperioso regular de manera pormenorizada su uso y la normativa procesal que habilite este tipo de medidas deberá limitarla para la investigación de un número cerrado de delitos graves. Asimismo, la falta de reglamentación legal no puede ser subsanada mediante una aplicación analógica de la regulación establecida respecto de otras medidas de investigación. Toda injerencia estatal que pueda afectar derechos constitucionales debe estar autorizada por una ley previa, clara y capaz de dar cuenta de las exigencias que deben ser acreditadas, controladas y satisfechas por una investigación que emplea

sistemas informáticos de vigilancia para cumplir con los estándares constitucionales de un debido proceso legal.

Antonella Bentín

(Ministerio Público de la Defensa)

El avance tecnológico y la ausencia de regulación en materia de prueba digital en Argentina, trae como consecuencia que los operadores judiciales utilicen como fundamento —entre otros— la Convención de Budapest sobre Ciberdelincuencia[1] y el principio de "libertad probatoria" para ordenar medidas de pruebas que, muchas veces, resultan invasivas de la privacidad de los ciudadanos[2].

Como lo explica Marcos Salt, los obstáculos que generan para la investigación penal los desarrollos de tecnologías informáticas han puesto en evidencia también la necesidad de regular este tipo de medios de investigación y, como contracara, prever las garantías y controles adecuados para que su uso no implique una afectación desproporcionada de los derechos fundamentales de los ciudadanos.

En el año 2022, el Alto Comisionado de las Naciones Unidas para los Derechos Humanos elaboró el informe "El derecho a la privacidad en la era digital". Se trata de un informe temático sobre cómo las herramientas digitales pueden emplearse contra las personas al exponerlas a nuevas formas de vigilancia, control y elaboración de perfiles y del impacto que ello genera en los derechos a la privacidad, intimidad, libertad de expresión y de opinión. Además, recomendó a los Estados que evaluaran el potencial impacto de sus actos en la población para desarrollar medidas de seguridad respetuosas de sus derechos humanos.

En el mismo sentido, el TEDH advirtió en varias sentencias que se desarrollarán a lo largo de este boletín (Ben Faiza v. Francia, Zoltán v. Eslovaquia, Saber v. Noruega), que la ley debe ser lo suficientemente clara para señalar en qué circunstancias y bajo qué condiciones se autoriza al Estado a realizar injerencias en la intimidad de las personas, más aun teniendo en consideración que los procedimientos técnicos utilizados se perfeccionan continuamente.

El hecho de tener una regulación clara permite garantizar —de algún modo— más transparencia en el proceso penal y asegura el derecho de defensa de la persona investigada.

Mientras tanto, ante la ausencia de una regulación, algunos operadores judiciales realizan aplicaciones analógicas de medios de pruebas convencionales. Es por ello, que desde el Ministerio Público de la Defensa —al igual que diversos organismos de DDHH especializados en la materia— observamos que frente a medidas de pruebas "novedosas" empiezan a ceder las garantías constitucionales de los ciudadanos, lo que merece especial atención.

Solo a modo de ejemplo, han surgido antecedentes jurisprudenciales a nivel nacional en los cuales se autorizó —mediante orden judicial— que el imputado desbloquee de manera "compulsiva" su dispositivo celular bajo el argumento que sería similar a la extracción de sangre de manera compulsiva prevista por los códigos procesales.

Disiento con la postura que afirma que se trata de medidas de pruebas asimilables o comparables: en primer lugar, porque el desbloqueo compulsivo de un celular no se encuentra previsto procesalmente, pero, además, el masivo contenido de un dispositivos celular —a diferencia de un análisis de ADN— puede involucrar a terceras personas, encontrarse pruebas de otros delitos, etc. El imputado no tiene el deber de colaboración por la ineficacia estatal de no poder desbloquear

[1] Convención sobre cibercrimen, disponible (en inglés) en https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

[2] Salt, Marcos. "Allanamiento remoto ¿Un cambio de paradigma en el registro y secuestro de datos informáticos?". En *Cibercrimen II*, 1a edición 2018. Ed. BdeF, pp. 151-181.

un dispositivo, ni de brindar pruebas que de otro modo no podrían obtener —a menos, claro está, que decida someterse al régimen de imputado colaborador—.

Este debate también será analizado en el precedente caso N° 4-19-70053 del Tribunal de Distrito Norte de California (EE. UU.), en el que se discutió si obligar a la imputada a otorgar su huella dactilar para desbloquear el dispositivo era violatorio de la Quinta Enmienda. Lo interesante de este precedente es que además realiza una distinción entre la comunicación verbal (por ejemplo, mencionar a viva voz una clave numérica) y el hecho de solamente aportar tus datos biométricos (huella, iris o rostro). Así, concluye que el escaneado de un dedo o pulgar utilizado para desbloquear un dispositivo indica que el dispositivo pertenece a una persona concreta. En otras palabras, el acto admite que el teléfono estaba en posesión y control del sospechoso, y autentifica la propiedad o el acceso al teléfono y a todo su contenido digital, lo que es violatorio de la quinta enmienda.

En un sentido similar, si desde la Defensa se observara que, en el marco de un procedimiento (por ejemplo, un allanamiento) el personal policial solicita al imputado el patrón de desbloqueo del dispositivo celular, ya sea bajo amenazas o sin asistencia letrada, esto debe ser fuertemente cuestionado con los mismos argumentos del fallo mencionado precedentemente.

No olvidemos que, debido a la gran capacidad de almacenamiento que caracteriza a los nuevos dispositivos electrónicos, se puede obtener un sinfín de información de la vida personal de las personas-fotos, videos, notas, aplicaciones varias con datos personales, entre otras- e inclusive, esa información puede ser de hace mucho tiempo atrás. Tal como se expresó en el fallo "Riley vs. California", en un teléfono celular se podría exponer a las autoridades mucho más que un exhaustivo allanamiento de un domicilio: un teléfono no solo contiene de forma digital muchos registros confidenciales encontrados previamente en el hogar; éste también contiene una amplia gama de información privada que nunca se encuentra en un domicilio.

Similares argumentos se establecieron en los precedentes "Jones" y "Carpenter" de la Corte Suprema de EE. UU., cuando se analizó la cantidad de datos sobre la vida privada que podía arrojar la geolocalización vinculada al teléfono celular de una persona determinada.

En ese sentido, es necesario resaltar que la vigilancia a través de dispositivos de seguimiento y localización constituye una de las medidas más intrusivas a la intimidad y privacidad de las personas, ya que permite un rastreo minucioso y sumamente detallado de todas sus actividades diarias y cotidianas, tal como se afirmó en el precedente "Carpenter vs. US".

Por este motivo deben extremarse y debe aplicarse con suma mesura este tipo de vigilancia sobre el imputado. La expectativa de privacidad se puede abordar desde dos aristas: por un lado, el derecho a preservar su ubicación física y movimientos y, por otro lado, la expectativa de privacidad de una persona respecto de la información entregada voluntariamente a terceros (por ejemplo, empresas privadas de telefonía, redes sociales, etc.).

Abordar la cuestión desde el derecho a la privacidad-y la protección de los datos personales- nos obliga entonces a delimitar, por ejemplo, cómo acceder a los datos de geolocalización que generó un determinado dispositivo o una plataforma digital, cómo se debe utilizar un dispositivo de seguimiento con geolocalización y durante qué tiempo, qué requisitos debe contener la orden judicial que lo autoriza, etc.

Mención aparte merece el momento de la incautación, preservación y análisis de evidencia digital —y su debida cadena de custodia—. En las investigaciones que involucran incautación de prueba digital exigen una planificación previa que permita determinar, por ejemplo, qué herramientas informáticas serán necesarias, qué tipo de información se buscará, cómo se realizará esa

búsqueda, se si secuestran los dispositivos electrónicos o si se realizará, o no, la extracción de la prueba digital en el lugar, entre otras cuestiones[3].

Como lo veremos en este boletín, al momento de extraer la información de un dispositivo electrónico, la defensa también debe prestar especial atención a que, previamente, se establezca el objeto y se delimite temporalmente qué información se buscará. Esto, en principio, podría evitar no solo una invasión desproporcionada a la intimidad de la persona, sino también los "hallazgos casuales" que no guardan vinculación con del delito investigado (Ver, por ejemplo, los fallos "United States v. Comprehensive Drug Testing", "United States v. Carey", o "Särgava V. Estonia" del TEDH).

Por todo lo expuesto, a fin de garantizar un equilibrio entre la persecución estatal y el derecho a la intimidad, resulta necesario que los operadores judiciales previamente realicen un análisis respecto a la necesidad, proporcionalidad e idoneidad de las medidas de pruebas en el marco de una investigación penal, como así también se evite flexibilizar las garantías constitucionales en pos de la eficacia estatal. Como ya lo mencioné, es sumamente importante que, así como se adaptaron las investigaciones a la nueva realidad tecnológica, también deben adaptarse las garantías de la persona imputada y no debe utilizarse "la libertad probatoria" como excusa para avasallar derechos reconocidos constitucionalmente.

Como reflexión final, me interesa resaltar que el trabajo interdisciplinario en esta temática resulta fundamental y es de vital importancia, ya que —en la mayoría de los casos— es totalmente necesaria la asistencia técnica para evaluar las diferentes situaciones con precisión. En ese sentido, se han creado fiscalías especializadas en ciberdelincuencia en las distintas provincias de la Argentina, las que cuentan con asistencia de peritos informáticos y/o asistencia de las fuerzas de seguridad especializadas en la temática, como así con herramientas informáticas de gran utilidad.

Por ello, a fin de aminorar esta desigualdad existente, desde el área de Capacitación de la Defensoría General de la Nación (Escuela de la Defensa Pública), se vienen brindado capacitaciones en torno a la temática —desde un punto de vista jurídico y también técnico— que fortalecen el servicio de justicia brindado.

Junto con los cursos, talleres y otras actividades de formación ofrecidos por la Escuela de la Defensa Pública, este boletín tiene por objeto visibilizar las distintas resoluciones favorables para la defensa en el ámbito tanto nacional como internacional sobre la prueba digital, que servirán de herramienta para la labor diaria de los Defensores como así también para continuar trabajando en futuros planteos.

[3] Delle Donne, Carla Paola. "La extracción de prueba electrónica de teléfonos celulares y la garantía de defensa en juicio". En *Dossier especial: el desafío de la prueba electrónica en el proceso judicial*. Ed. Thomson Reuters.

1. DESBLOQUEO COMPULSIVO DE DISPOSITIVOS ELECTRÓNICOS

JURISPRUDENCIA INTERNACIONAL

1.1. TRIBUNAL DE DISTRITO DE LOS ESTADOS UNIDOS, DISTRITO NORTE DE CALIFORNIA. "ORDEN POR LA QUE SE DENIEGA LA SOLICITUD DE UNA ORDEN DE REGISTRO". CASO N° 4-19-70053. 10/06/2019.

HECHOS

Dos personas fueron investigadas por su presunta participación en un caso de "sextorsión", utilizando Facebook Messenger para amenazar a una víctima con la distribución de un video íntimo si no pagaba. Debido a esta situación, la Fiscalía solicitó una orden de registro con el propósito de incautar elementos relacionados con el presunto delito. En su solicitud, la Fiscalía requirió que se incluyeran dispositivos electrónicos, en un domicilio ubicado en Oakland, California. Contra ese pedido, la defensa solicitó una contrarréplica de lo requerido por la Fiscalía. Para ello, sostuvo que la exigencia de desbloquear dispositivos electrónicos mediante huella dactilar o reconocimiento facial eran contrarias a las Enmiendas Cuarta y Quinta de la Constitución de Estado Unidos que protegen contra registros y secuestros irrazonables y garantizan el derecho contra la autoincriminación, respectivamente. Además, que la exigencia de desbloquear dispositivos mediante métodos biométricos constituiría un testimonio autoincriminatorio protegido por la Quinta Enmienda, ya que revelaría información personal que podría utilizarse en su contra en un proceso penal. Finalmente, que la medida requerida era intrusiva y desproporcionada, toda vez que el desbloqueo biométrico trascendía los límites de la evidencia física, afectando la esfera privada y la protección de datos personales.

DECISIÓN

El Tribunal del Distrito Norte de California rechazó la orden de registro solicitada por el gobierno. Para ello, consideró que el gobierno no puede obligar o utilizar de otro modo dedos, pulgares, reconocimiento facial, óptico/iris, o cualquier otra característica biométrica para desbloquear dispositivos electrónicos.

ARGUMENTOS

1. Derecho a la privacidad. Política criminal. Orden judicial. Decomiso. Razonabilidad. Control judicial. Principio de proporcionalidad. Datos biométricos. Protección de datos personales. Sistema informático. Telefonía celular. Declaración jurada.

"La Cuarta Enmienda protege ´el derecho de las personas a estar seguras en sus personas, casas, papeles y efectos, contra registros e incautaciones irrazonables´. En ese sentido, ´El ´propósito básico de esta Enmienda´, han reconocido nuestros casos, ´es salvaguardar la privacidad y la seguridad de los individuos contra invasiones arbitrarias por parte de funcionarios gubernamentales´´. Ver *Carpenter v. United States*".

"Hay suficientes hechos en la declaración jurada para creer que se encontrarán pruebas del delito en los locales objeto de la investigación, por lo que el gobierno tiene una causa probable para llevar a cabo un registro legal, siempre y cuando se ajuste a la Cuarta Enmienda, Sin embargo, si la aplicación de la ley viola otro derecho constitucional en el curso de la ejecución de una orden judicial, inherentemente hace que el registro y la incautación sean irrazonables".

“Además del registro de los locales, el gobierno solicita una orden que permita a los agentes que ejecutan esta orden obligar a ´cualquier individuo, que se encuentre en los locales objeto de la orden y que las fuerzas del orden crean razonablemente que es un usuario del dispositivo, a desbloquear el dispositivo utilizando características biométricas...´. Esta petición es excesiva. Hay dos sospechosos identificados en la declaración jurada, pero la solicitud no se limita a una persona concreta ni a un dispositivo concreto”.

“[L]a Corte considera que la solicitud no establece una causa probable suficiente para obligar a cualquier persona que se encuentre en los locales en cuestión en el momento del registro a proporcionar un dedo, pulgar u otra característica biométrica para desbloquear potencialmente cualquier dispositivo digital no especificado que pueda ser incautado durante el registro, por lo demás legal”.

“[L]a solicitud del Gobierno de registrar e incautar todos los dispositivos digitales en los locales objeto de la investigación es igualmente excesiva. No se puede permitir que el Gobierno registre e incaute un teléfono móvil u otro dispositivo que se encuentre en la persona de un no sospechoso simplemente porque esté presente durante un registro legal”.

“Mientras se deniegue la orden, cualquier nueva presentación deberá limitarse a aquellos dispositivos que las fuerzas del orden crean razonablemente que son propiedad o están bajo el control de los dos sospechosos identificados en la declaración jurada”.

“Incluso si existe causa probable para incautar los dispositivos localizados durante un registro legal basado en la creencia razonable de que pertenecen a un sospechoso, la causa probable no permite al gobierno obligar a un sospechoso a renunciar a los derechos que de otro modo le otorga la Constitución, incluido el derecho de la Quinta Enmienda contra la autoincriminación. La Quinta Enmienda establece que ninguna persona ´será obligada en ningún caso penal a declarar contra sí misma´. La investigación apropiada es si un acto requeriría la compulsión de una comunicación testimonial incriminatoria. Véase *Fisher v. United States*. En este caso, la cuestión es si el uso de la característica biométrica de un sospechoso para desbloquear potencialmente un dispositivo electrónico es testimonial en virtud de la Quinta Enmienda”.

“El reto al que se enfrentan los tribunales es que la tecnología va por delante de la ley. En reconocimiento de esta realidad, la Corte Suprema de los Estados Unidos ha dado recientemente instrucciones a los tribunales para que adopten normas que ´tengan en cuenta los sistemas más sofisticados que ya están en uso o en desarrollo´. Véase *Carpenter* (citando *Kyllo v. United States*). Los tribunales tienen la obligación de salvaguardar los derechos constitucionales y no pueden permitir que esos derechos se vean mermados por el mero avance de la tecnología. Véase *Carpenter* (citando *Kyllo*) (La Corte Suprema de los Estados Unidos ha tratado repetidamente de ´asegurar la preservación de ese grado de privacidad frente al gobierno que existía cuando se adoptó la Cuarta Enmienda´). Los ciudadanos no contemplan renunciar a sus derechos civiles cuando utilizan nuevas tecnologías, y la Corte Suprema ha llegado a la conclusión de que, considerar lo contrario, dejaría a los individuos ´a merced del avance de la tecnología´. Véase *Carpenter*”.

“Aunque la seguridad de los dispositivos digitales no es un concepto nuevo, los medios para hacerlo han cambiado. De hecho, los consumidores han tenido la posibilidad de utilizar códigos numéricos o alfanuméricos para bloquear sus dispositivos durante décadas. Los tribunales que han abordado la cuestión del código de acceso han dictaminado que éste no puede ser obligado en virtud de la Quinta Enmienda, porque el acto de comunicar el código de acceso es testimonial, ya que ´la expresión del contenido de la mente de una persona entra de lleno en la protección de la Quinta Enmienda´. Véase *Doe v. United States* (Stevens, J., disidente) (citando *Boyd v. United*

States; *Fisher v. United States*; véase también *United States v. Kirschner* (citando *Doe*); *Com. v. Baust*. Hoy en día, la tecnología ha proporcionado a los ciudadanos atajos para introducir códigos de acceso mediante la utilización de características biométricas. La cuestión, por tanto, es si se puede obligar a un sospechoso a utilizar su dedo, pulgar, iris u otra característica biométrica para desbloquear un dispositivo digital".

"El testimonio no se limita a las comunicaciones verbales o escritas. Los actos que implican afirmaciones de hecho pueden constituir comunicación testimonial a los efectos de la Quinta Enmienda. Véase *Doe*. Específicamente, el ´acto mismo de producción de un testigo podría calificarse como testimonial si conceder la existencia, posesión y control, y autenticidad de los documentos tendiera a incriminarlos´. In re *Grand Jury Subpoena Duces Tecum* (citando *Fisher*)".

"No obstante, ciertos actos, aunque incriminatorios, no están amparados por el privilegio, como proporcionar una muestra de sangre, someterse a la toma de huellas dactilares, proporcionar un ejemplar de escritura o voz, o presentarse en una rueda de reconocimiento. Véase *Doe*. La distinción que ha surgido, a menudo expresada de diferentes maneras, es que el privilegio es un impedimento para obligar a las ´comunicaciones o al ´testimonio´, pero que la compulsión que hace que un sospechoso o un acusado se conviertan en fuente de ´pruebas reales o físicas´ no lo viola´. Véase *Schmerber v. California*; véase también *Doe v. United States*".

"La Corte Suprema considera que la utilización de una función biométrica para desbloquear un dispositivo electrónico no es similar a someterse a una toma de huellas dactilares o a una muestra de ADN, porque difiere en dos aspectos fundamentales. En primer lugar, el gobierno admite que un dedo, el pulgar u otra característica biométrica se puede utilizar para desbloquear un dispositivo en lugar de un código de acceso. En este contexto, las características biométricas sirven para el mismo propósito que un código de acceso, que es asegurar el contenido del propietario, lo que las hace funcionalmente equivalentes. Como reconoce el gobierno, hay ocasiones en las que el dispositivo no aceptará la función biométrica y requerirá que el usuario teclee el código de acceso para desbloquear el dispositivo. Por ejemplo, el código de acceso suele ser necesario ´cuando el dispositivo se ha reiniciado, está inactivo o no se ha desbloqueado durante un cierto periodo de tiempo´. Se trata, sin duda, de una medida de seguridad para garantizar que alguien sin el código de acceso no pueda acceder fácilmente al contenido del teléfono. De hecho, el gobierno expresa cierta urgencia con la necesidad de obligar al uso de las funciones biométricas para evitar la necesidad de introducir un código de acceso. Esta urgencia parece tener su origen en la incapacidad del gobierno para obligar a la producción de la contraseña en virtud de la jurisprudencia actual. De ello se deduce, sin embargo, que, si no se puede obligar a una persona a proporcionar una contraseña porque se trata de una comunicación testimonial, no se puede obligar a una persona a proporcionar su dedo, pulgar, iris, rostro u otra característica biométrica para desbloquear ese mismo dispositivo".

"En segundo lugar, pedir a alguien que coloque su dedo o pulgar en un dispositivo digital es fundamentalmente diferente a pedir a un sospechoso que se someta a una toma de huellas dactilares. El escaneado de un dedo o pulgar utilizado para desbloquear un dispositivo indica que el dispositivo pertenece a una persona concreta. En otras palabras, el acto admite que el teléfono estaba en posesión y control del sospechoso, y autentifica la propiedad o el acceso al teléfono y a todo su contenido digital. Así pues, el acto de desbloquear un teléfono con un escáner dactilar o pulgar supera con creces las ´pruebas físicas´ creadas cuando un sospechoso se somete a una toma de huellas dactilares para comparar simplemente sus huellas dactilares con las pruebas físicas existentes (otra huella dactilar) encontradas en la escena de un delito, porque no se requiere comparación ni corroboración por testigos para confirmar una coincidencia positiva. En su lugar, un escaneado dactilar o pulgar satisfactorio confirma la propiedad o el control del dispositivo y, a diferencia de las huellas dactilares, la autenticación de su contenido no puede

refutarse razonablemente. En una situación similar, la Corte Suprema in re *Application for a Search Warrant* observó que ´con un simple toque de dedo, el sospechoso está testificando que ha accedido al teléfono antes, como mínimo, para configurar las funciones de contraseña de huellas dactilares, y que actualmente tiene cierto nivel de control o una conexión relativamente importante con el teléfono y su contenido´. También es digno de mención que muchas aplicaciones de teléfonos inteligentes que proporcionan acceso a información personal y privada —incluidos registros médicos y cuentas financieras— ahora permiten a los usuarios utilizar funciones biométricas en lugar de códigos de acceso para acceder a esos registros. Como observó astutamente el juez Weisman, utilizar una huella dactilar para situar a alguien en un lugar concreto es un escenario totalmente distinto que utilizar un escáner dactilar ´para acceder a una base de datos con la información más privada de alguien´. In re *Application for a Search Warrant*. Por lo tanto, el que suscribe considera que un rasgo biométrico es análogo a las respuestas fisiológicas no verbales obtenidas durante una prueba de polígrafo, que se utilizan para determinar la culpabilidad o la inocencia, y se consideran testimoniales. Véase S*chmerher*".

"Aunque este Tribunal simpatiza con el interés del gobierno en acceder al contenido de cualquier dispositivo electrónico que pueda incautar legalmente, hay otras formas en que el gobierno puede acceder al contenido que no pisotean la Quinta Enmienda. En el presente caso, el gobierno puede obtener cualquier comunicación de Facebook Messenger de Facebook en virtud de la *Stored Communications Act* o de una orden judicial basada en una causa probable. Si bien puede ser más conveniente eludir Facebook, e intentar obtener acceso infringiendo el privilegio de la Quinta Enmienda contra la autoincriminación, es un abuso de poder y es inconstitucional. El hecho de que el gobierno nunca pueda acceder al contenido completo de un dispositivo digital no afecta al análisis".

"La doctrina de la conclusión anticipada es una aplicación de la Quinta Enmienda ´mediante la cual el gobierno puede demostrar que no se cuestiona ningún testimonio´. In re, *Grand Jury Subpoena Duces Tecum*. Específicamente, ´cuando la ´existencia y ubicación´ de los documentos bajo citación son una ´conclusión previsible´ y el testigo ´agrega poco o nada a la suma total de la información del Gobierno al conceder que de hecho tiene los [documentos]´, entonces no se toca ningún derecho de la Quinta Enmienda porque la ´cuestión no es de testimonio sino de entrega´´. In re, *Grand Jury Subpoena* (citando *Fisher v. United States*)".

"[L]a respuesta de un testigo a una citación judicial destinada a obtener pruebas potencialmente incriminatorias es testimonial. Véase *Estados Unidos v. Hubbell*. La doctrina de la conclusión previsible no se aplica cuando el gobierno no puede demostrar el conocimiento previo de la existencia o el paradero de los documentos presentados en última instancia en respuesta a una citación".

"Los teléfonos móviles actuales no son comparables a otros equipos de almacenamiento, ya sean físicos o digitales, y tienen derecho a una mayor protección de la intimidad. Véase *Riley v. California* (Un smartphone desbloqueado no puede ser registrado con ocasión de una detención más que para determinar si puede ser utilizado como arma); véase también *Carpenter*. Al llegar a esta conclusión, la Corte Suprema reconoció que los teléfonos inteligentes son miniordenadores con capacidad para realizar llamadas telefónicas, cuyo registro ´normalmente expondría al gobierno mucho más que el registro más exhaustivo de una casa: Un teléfono no sólo contiene en forma digital muchos registros sensibles que antes se encontraban en el hogar; también contiene una amplia gama de información privada que nunca se encuentra en un hogar de ninguna forma, a menos que el teléfono esté presente´. Véase *Riley*. Además, ´en el contexto del teléfono móvil... es razonable esperar que se encuentre información incriminatoria en un teléfono con independencia de cuándo se produzca el delito´. Por lo tanto, los teléfonos móviles están

sujetos a un tratamiento diferente al de los dispositivos de almacenamiento más tradicionales, como las cajas fuertes, y deben gozar de mayor protección".

"De ello se deduce que cualquier argumento que sostenga que obligar a un sospechoso a proporcionar una característica biométrica para acceder a documentos y datos es sinónimo de presentar documentos en virtud de una citación judicial fracasaría. Como reconoció la Corte Suprema en el caso *Riley*, los teléfonos inteligentes contienen grandes cantidades de datos, incluidos datos de localización GPS y registros confidenciales, cuyo contenido íntegro no puede ser anticipado por las fuerzas del orden. Véase *Riley*. En consecuencia, el gobierno carece intrínsecamente del conocimiento previo necesario de la información y los documentos que podría obtener mediante un registro de estos dispositivos digitales desconocidos, de modo que no sería una cuestión de mera entrega. Véase *Hubbell*. Además, el gobierno sería incapaz de articular hechos para obligar al desbloqueo de dispositivos que utilizan características biométricas por parte de personas desconocidas que el gobierno no podría prever que estuvieran presentes durante la ejecución de la orden de registro. De hecho, el pedido del registro de la fiscalía no hace ningún intento de hacerlo".

1.2. CORTE SUPREMA DEL ESTADO DE INDIANA. "KATELIN EUNJOO SEO V. ESTADO DE INDIANA". EXPEDIENTE N° 18S-CR-595. 23/6/2020.

HECHOS

Una mujer presentó una denuncia contra otra persona, identificada como D.S., y permitió a un detective revisar su dispositivo móvil como evidencia. Tras analizar las comunicaciones y entrevistar a la denunciante, no se presentaron cargos contra D.S., sino que la investigación reveló que la mujer había contactado primero a D.S. desde su propio número y luego continuó el acoso de forma anónima. Como resultado, se emitió una orden de detención contra la denunciante. Al ser detenida, la policía confiscó su dispositivo móvil bloqueado. Cuando se le pidió que proporcionara la contraseña, la mujer se negó, lo que llevó a obtener dos órdenes de registro: una para una descarga forense del teléfono en busca de pruebas y otra para obligarla a desbloquearlo bajo amenaza de desacato judicial. Después de negarse nuevamente, se solicitó que se la declarara en rebeldía. La defensa alegó que obligarla a desbloquear el dispositivo violaba su derecho a no autoincriminarse según la Quinta Enmienda. Sin embargo, el tribunal determinó que desbloquear el teléfono no constituía autoincriminación. Se interpuso un recurso de apelación contra esta decisión, y la orden de desacato fue suspendida mientras se resolvía. Mientras tanto, la mujer llegó a un acuerdo con el Estado, declarándose culpable de acoso y desestimando otros cargos. A pesar del acuerdo, la orden de rebeldía seguía vigente, lo que la exponía a posibles sanciones por desobedecerla.

DECISIÓN

La Corte Suprema del Estado de Indiana decidió que el gobierno violó los derechos de la Quinta Enmienda y revocó la orden de rebeldía.

ARGUMENTOS

1. Intervención de las telecomunicaciones. Prueba. Prueba digital. Telefonía celular. Debida diligencia. Debido proceso. Orden judicial.

"Extender la excepción de la conclusión previsible a la producción obligatoria de un teléfono inteligente desbloqueado genera preocupación por tres razones: tal expansión (1) no tiene en cuenta la ubicuidad y capacidad únicas de los teléfonos inteligentes; (2) puede resultar inviable; y (3) va en contra de los precedentes de la Corte Suprema de EE. UU. [...]".

"Los teléfonos inteligentes están en todas partes y lo contienen todo. Se han convertido en una ´parte tan omnipresente e insistente de la vida cotidiana que el proverbial visitante de Marte podría concluir que son una característica importante de la anatomía humana´. Ver *Riley v. California*. De hecho, un informe de 2019 del Centro de Investigaciones Pew reveló que el 81% de los estadounidenses posee un teléfono inteligente, frente al 35% en 2011. La Corte Suprema en [los casos] *Fisher*, *Doe* o *Hubbell* seguramente no podía haber previsto que tales dispositivos llegarían a ser tan comunes o imaginado la amplitud y profundidad de la información que podrían contener".

"Notablemente, en cada uno de esos casos, una citación limitó la información implicada por la producción obligada. En *Fisher* reconoció este alcance limitado, afirmando que las citaciones buscaban ´documentos de incuestionable relevancia para la investigación fiscal´, pero que ´la citación de un diario personal podría plantear problemas especiales de privacidad´. La Corte en *Doe* señaló que los documentos obligados, que ´pertenecían a las empresas del demandado´, eran menos personales que los solicitados en *Fisher,* que ´se referían a las declaraciones de impuestos individuales de los contribuyentes´. Sin embargo, un smartphone desbloqueado contiene mucha

más información privada de la que podría contener un diario personal o una declaración de la renta individual. Sin embargo, cuando se obliga a los sospechosos a entregar sus teléfonos inteligentes desbloqueados, no existe un limitador como una citación documental para archivos específicos".

"El caso *Hubbell* ilustra además la considerable diferencia entre cumplir una orden judicial de presentar un smartphone desbloqueado y cumplir una citación documental. Recordemos que, en *Hubbell*, el Gobierno no había demostrado que tuviera conocimiento previo de la existencia o ubicación de 13.120 páginas de documentos. Aunque no es una cantidad insignificante de información, palidece en comparación con lo que se puede almacenar en los smartphones actuales. De hecho, el modelo más barato del smartphone más vendido del año pasado, con una capacidad de 64 gigabytes de datos, puede almacenar más de 4.000.000 de páginas de documentos, más de 300 veces el número de páginas producidas en *Hubbell*. No es exagerado describir el código de acceso de un smartphone como ´la proverbial 'llave del reino de un hombre'´".

2. Sistema informático. Derecho a la intimidad. Derecho a la privacidad. Telefonía celular. Prueba. Prevención e investigación.

"Esto nos lleva a una segunda preocupación sobre la ampliación de la excepción de conclusión previsible: puede resultar inviable en este contexto. Los smartphones actuales ´podrían llamarse cámaras, reproductores de vídeo, agenda de contactos, calendarios, grabadoras, bibliotecas, agendas, álbumes, televisores, mapas o periódicos´. Y pueden contener, en forma digital, la ´huella combinada de lo que ha estado ocurriendo social, económica, personal, psicológica, espiritual y a veces incluso sexualmente, en la vida del propietario´".

"Reconociendo estas realidades, varios tribunales han determinado que el gobierno —antes de obligar a un sospechoso a desbloquear su teléfono inteligente— debe identificar específicamente los archivos que busca con una particularidad razonable. Pero incluso entonces, el gobierno debe tener acceso sólo a esos archivos. Sin embargo, obligar a presentar un teléfono inteligente desbloqueado da al gobierno acceso a todo lo que hay en el dispositivo, no sólo a los archivos que puede identificar con ´particularidad razonable´. Por ejemplo, aquí, incluso si el Estado pudiera demostrar que conocía y podía identificar archivos específicos en el *iPhone* de Seo, no hay nada que restrinja el acceso de las fuerzas del orden sólo a esa información. Después de todo, la orden autorizaba el registro del dispositivo de Seo sin limitación alguna".

"Ese acceso ilimitado a posibles pruebas en su *iPhone* —o en cualquier smartphone— plantea varias cuestiones complejas. Por ejemplo, si los agentes que registran el smartphone de un sospechoso encuentran una aplicación o un sitio web protegido por otra contraseña, ¿necesitarán una petición aparte para obligar al sospechoso a desbloquear esa aplicación o sitio web? ¿Y se aplicaría también la excepción de conclusión previsible a ese acto de producción? Supongamos que las fuerzas de seguridad abren una aplicación o un sitio web y la contraseña se rellena automáticamente. ¿Pueden los agentes acceder legalmente a esa información? ¿Y si un sospechoso tiene un servicio de almacenamiento en la nube —como *iCloud* o *Dropbox*— instalado en el dispositivo, que podría contener cientos de miles de archivos? ¿Pueden las fuerzas del orden consultar esos documentos, aunque esta ganancia equivaldría a identificar la ubicación de un almacén cerrado que los agentes aún no sabían que existía? Tal complejidad no es necesaria ni sorprendente: la excepción de conclusión previsible es, en este contexto, una clavija de baja tecnología en un agujero de vanguardia".

3. Telefonía celular. Almacenamiento. Orden judicial. Derecho a la intimidad. Patrimonio. Autoincriminación.

“Esto nos lleva a una tercera preocupación sobre la ampliación de la excepción de conclusión previsible: parece imprudente a la luz de la reciente jurisprudencia de la Corte Suprema relativa a los smartphones y la aplicación limitada y cuestionable de la excepción. La Corte Suprema ha dudado a la hora de aplicar incluso doctrinas arraigadas a dilemas novedosos, totalmente imprevistos cuando se crearon esas doctrinas. De hecho, el Tribunal observó recientemente que, al ´enfrentar nuevas preocupaciones forjadas por la tecnología digital´, ´ha tenido cuidado de no extender acríticamente los precedentes existentes´. Véase *Carpenter v. United States*. A ese punto, cuatro años antes, en *Riley*, el Tribunal sostuvo que la excepción de búsqueda-incidente-arresto al requisito de orden judicial no se extiende a un teléfono celular encontrado a una persona detenida. Y en *Carpenter*, el Tribunal sostuvo que la doctrina de terceros no se extiende a la información de localización de sitios celulares, al menos cuando se obtienen datos de siete días. La negativa de la Corte Suprema a ampliar estas dos doctrinas establecidas —cada una de ellas mucho más arraigada que la excepción de conclusión previsible— es instructiva”.

“Aunque *Riley* y *Carpenter* se decidieron en virtud de la Cuarta Enmienda, la preocupación del Tribunal en cada caso fue con los ´intereses de privacidad´ implicados por los teléfonos inteligentes, véase *Riley*. Y esa preocupación por la intimidad se aplica igualmente al privilegio de la Quinta Enmienda contra la autoincriminación. Aunque este privilegio no es ´ un protector general de la intimidad´, en el caso *Fisher* se reconoció que ´sirve verdaderamente a los intereses de la intimidad´ al proteger a los sospechosos de ser obligados a prestar testimonio privado y autoincriminatorio”.

“La aplicación limitada y cuestionable de la excepción de conclusión previsible también desaconseja ampliarla. De hecho, en *Fisher* se decidió hace más de cuarenta y cuatro años, y sigue siendo la única decisión de la Corte Suprema de EE. UU. en la que se considera aplicable la excepción. En los años transcurridos desde entonces, el Tribunal la ha debatido en dos ocasiones y en un único contexto: en los procedimientos del gran jurado, cuando una citación obligaba a presentar documentos comerciales y financieros. Durante este mismo período de tiempo, los juristas —incluidos tres miembros actuales de la Corte Suprema— se han preguntado si en *Fisher* interpretó la Quinta Enmienda de forma demasiado restrictiva, poniendo en tela de juicio la viabilidad de la propia excepción de conclusión anticipada. Independientemente de la viabilidad de la excepción de conclusión previsible, parece imprudente extenderla más allá de su aplicación única. *Cf. Silverman v. United States* (decidiendo no extender el razonamiento de un caso factualmente distinto ‘ni siquiera por una fracción de pulgada’)”.

“No es de extrañar que los tribunales que han abordado recientemente esta cuestión —cómo se aplica la Quinta Enmienda a la presentación forzosa de dispositivos electrónicos desbloqueados— se hayan negado a ampliar la excepción de conclusión inevitable o no la hayan mencionado en absoluto. La excepción no sólo se elaboró para un contexto muy diferente, sino que su ampliación supondría extender una excepción legal de hace décadas y definida de forma restrictiva a una tecnología en desarrollo dinámico que estaba en pañales hace tan sólo una década. Y también supondría limitar un derecho constitucional. Sin embargo, aunque hemos identificado tres problemas que plantea la ampliación de la excepción de conclusión previsible a este contexto, no necesitamos pronunciarnos de forma general sobre su validez porque sencillamente no es aplicable en este caso”.

“Al mismo tiempo, hacemos hincapié en que hay varias formas en que las fuerzas del orden pueden obtener pruebas de los teléfonos inteligentes sin infringir los derechos de la Quinta Enmienda de una persona. Por ejemplo, los agentes podrían tratar de obtener información de terceros en virtud de la Ley de Comunicaciones Almacenadas. Alternativamente, dos empresas —*Cellebrite* y *Grayshift*— ofrecen a los organismos encargados de hacer cumplir la ley productos asequibles que proporcionan acceso a un teléfono inteligente bloqueado. O los oficiales podrían solicitar una orden que obligue al fabricante del teléfono inteligente a ayudar a eludir la pantalla

de bloqueo. Y si las fuerzas de seguridad quieren acceder a un teléfono inteligente por razones distintas de la persecución, pueden ofrecer inmunidad al propietario del dispositivo. Véase [el caso] *Doe* . Pero el Estado no puede pescar pruebas incriminatorias obligando a Seo a dar acceso sin restricciones a su *iPhone* cuando no ha demostrado que exista ningún archivo en el smartphone de Seo o que ella poseyera esos archivos".

"Hace casi un siglo, el juez Louis Brandeis de la Corte Suprema de los EE. UU. advirtió: ´Algún día pueden desarrollarse medios por los que el gobierno, sin sacar papeles de los cajones secretos, pueda reproducirlos en el tribunal, y por los que estará capacitado para exponer ante un jurado los sucesos más íntimos del hogar´. Véase *Olmstead v. United States* (Brandeis, J., disidente). Ese día ha llegado. Y permitir que el Estado, en estos hechos, obligue a Seo a desbloquear su *iPhone* para la aplicación de la ley inclinaría la balanza demasiado a favor del Estado, dando lugar a una erosión sísmica del privilegio de la Quinta Enmienda contra la autoincriminación. No lo haremos".

2. GEOLOCALIZACIÓN, VIGILANCIA ELECTRÓNICA E INTERCEPTACIÓN DE COMUNICACIONES

JURISPRUDENCIA INTERNACIONAL

2.1. CORTE SUPREMA DE JUSTICIA DE LOS ESTADOS UNIDOS "UNITED STATES V. JONES". 23/01/2012.

HECHOS

En el marco de una investigación criminal, personal de la Oficina Federal de Investigación (FBI —sigla en inglés—) obtuvo una orden judicial para instalar un dispositivo de geolocalización (GPS —sigla en inglés—) en el automóvil estacionado en un lugar público de una persona sospechosa de tráfico de estupefacientes. La orden judicial autorizaba la instalación del GPS en el Distrito de Columbia y dentro del plazo de diez días. Sin embargo, los agentes instalaron el dispositivo el día undécimo en el Estado de Maryland. Posteriormente, las autoridades federales siguieron los movimientos del vehículo durante veintiocho días. Como resultado de esa investigación, a la persona se le secuestró aproximadamente cinco kilogramos de cocaína, fue detenido e imputado por los delitos de conspiración y tráfico de estupefacientes. Previo al juicio, su defensa solicitó la nulidad de las pruebas obtenidas mediante el dispositivo GPS. El tribunal federal de primera instancia condenó a la persona. Para ello, descartó los datos del GPS que habían sido obtenidos mientras el automóvil se encontraba en la casa de la persona imputada. Sin embargo, admitió el resto de los datos obtenidos al considerar que una persona que viaja en un automóvil por la vía pública no tiene ninguna expectativa razonable de privacidad en sus movimientos de un lugar a otro. Posteriormente, un gran jurado presentó otra acusación contra él un grupo de personas por el mismo delito. En esa instancia, el representante del gobierno presentó los mismos datos de localización obtenidos por GPS admitidos en el primer juicio que conectaba a todos los involucrados. El jurado emitió un veredicto de culpabilidad y el tribunal condenó a la persona a cadena perpetua. Por su parte, el Tribunal de Apelaciones para el Distrito de Columbia revocó la sentencia y consideró que la admisión de las pruebas obtenidas mediante el uso del dispositivo GPS sin orden judicial era contraria a la IV Enmienda de la Constitución de los Estados Unidos. Para ello, diferenció entre el seguimiento de un auto durante un único viaje y el seguimiento de todos los viajes de la persona en el transcurso de un mes.

DECISIÓN

La Corte Suprema de Justicia de los Estados Unidos decidió que la instalación del dispositivo GPS en el vehículo, ordenada por el Gobierno, y la utilización de ese recurso para controlar los movimientos del automóvil constituyen un registro en los términos de la Cuarta Enmienda. La opinión del Tribunal estuvo a cargo del ministro Scalia (adhesión de los ministros Roberts, Kennedy y Sotomayor), y los votos concurrentes por separado de los ministros Alito (con la adhesión de los ministros Ginsburg, Breyer y Kagan) y Sotomayor, respectivamente.

ARGUMENTOS

1. Razonabilidad. Vigilancia electrónica. Derecho a la privacidad. Derecho a la intimidad. Derecho a la privacidad. Prueba. Prueba digital. Almacenamiento. Política criminal.

"La Cuarta Enmienda establece en su parte pertinente que ´no se violará el derecho del pueblo a la seguridad de sus personas, hogares, documentos y efectos personales, contra registros e incautaciones irrazonables´. Es indiscutible que un vehículo es un ´efecto´ en el sentido en que se utiliza este término en la Enmienda. La instalación por parte del Gobierno de un dispositivo GPS

en el vehículo de un objetivo y el uso de dicho dispositivo para vigilar los movimientos del vehículo constituye un ´registro´" (opinión de Scalia, adhesión de Roberts, Kennedy y Sotomayor).

"El Gobierno ocupó físicamente una propiedad privada con el fin de obtener información. No tenemos ninguna duda de que tal intrusión física habría sido considerada un ´registro´ en el sentido de la Cuarta Enmienda cuando fue adoptada. En *Brower v. County of Inyo* (citando *Boyd v. United States*), Lord Camden expresó en términos claros la importancia de los derechos de propiedad en el análisis del registro y la incautación: ´[N]uestra ley considera la propiedad de todo hombre tan sagrada que nadie puede poner el pie en el terreno de su vecino sin su permiso; si lo hace, es un intruso, aunque no cause ningún daño; si pisa el terreno de su vecino, debe justificarlo por ley´" (opinión de Scalia, adhesión de Roberts, Kennedy y Sotomayor).

"El texto de la Cuarta Enmienda refleja su estrecha relación con la propiedad, ya que de lo contrario se habría referido simplemente al ´derecho del pueblo a estar seguro contra registros e incautaciones irrazonables´; la frase ´en sus personas, casas, papeles y efectos´ hubiera sido superflua. En *Olmstead v. United States*, se sostuvo que las escuchas telefónicas conectadas a cables telefónicos en la vía pública no constituían un registro en virtud de la Cuarta Enmienda porque ´[n]o se entró en las casas u oficinas de los acusados´" (opinión de Scalia, adhesión de Roberts, Kennedy y Sotomayor).

"Casos posteriores, por supuesto, se han desviado de ese enfoque basado exclusivamente en la propiedad. En *Katz v. United States*, se sostuvo que ´la Cuarta Enmienda protege a las personas, no a los lugares´, y encontramos una violación en la colocación de un dispositivo de escucha en una cabina telefónica pública. Casos posteriores han aplicado el análisis de la concurrencia del Juez Harlan en ese caso, que dijo que se produce una violación cuando los funcionarios del gobierno violan la ´expectativa razonable de privacidad´ de una persona. Véase, por ejemplo, *Bond v. United States*; *California v. Ciraolo*; *Smith v. Maryland*" (opinión de Scalia, adhesión de Roberts, Kennedy y Sotomayor).

"El Gobierno sostiene que la norma Harlan demuestra que aquí no hubo registro, ya que Jones no tenía una ´expectativa razonable de privacidad´ en la zona de su vehículo a la que accedieron los agentes del Gobierno (sus bajos) y en la ubicación del vehículo en la vía pública, que era visible para todos. Pero no necesitamos abordar los argumentos del Gobierno, porque los derechos de Jones en virtud de la Cuarta Enmienda no aumentan o disminuyen con la formulación de[l caso] *Katz*. En el fondo, debemos ´asegurar la preservación del grado de privacidad frente al gobierno que existía cuando se adoptó la Cuarta Enmienda´. Durante la mayor parte de nuestra historia se entendió que la Cuarta Enmienda incorporaba una preocupación particular por la intrusión del gobierno en las áreas (´personas, casas, papeles y efectos´) que enumera. En el caso *Katz* no se repudió esa interpretación. Menos de dos años después, el Tribunal confirmó el argumento de los acusados de que el Gobierno no podía presentar contra ellos conversaciones entre otras personas obtenidas mediante la colocación sin orden judicial de dispositivos de vigilancia electrónica en sus domicilios. La opinión rechazó el argumento del disidente de que no había violación de la Cuarta Enmienda ´a menos que se invadiera la intimidad conversacional del propio propietario de la vivienda´. ´[N]o creemos que [en el caso] *Katz*, al sostener que la Cuarta Enmienda protege a las personas y sus conversaciones privadas, pretendiera retirar ninguna de las protecciones que la Enmienda extiende al hogar...´" (opinión de Scalia, adhesión de Roberts, Kennedy y Sotomayor).

"En *Soldal v. Cook County*, el Tribunal rechazó unánimemente el argumento de que, aunque se había producido una ´incautación´ ´en un sentido 'técnico'´ cuando se retiró por la fuerza una casa remolque, no se había violado la Cuarta Enmienda porque las fuerzas del orden no habían ´invadido la intimidad [de las personas]´. El Tribunal explicó que en el caso *Katz* se estableció que ´los derechos de propiedad no son la única medida de la Cuarta Enmienda´. En *Katz*, el Tribunal estableció que ´los derechos de propiedad no son la única medida de las violaciones de la Cuarta

Enmienda´, pero no ´la protección de la propiedad anteriormente reconocida´. Como explicó el Juez Brennan en su concurrencia en *Knotts*, [el caso] *Katz* no erosionó el principio ´de que, cuando el Gobierno realiza una intrusión física en una zona constitucionalmente protegida para obtener información, esa intrusión puede constituir una violación de la Cuarta Enmienda´. Hemos plasmado esa preservación de los *pastrights* en nuestra propia definición de ´expectativa razonable de privacidad, que hemos dicho que es una expectativa ´que tiene una fuente fuera de la Cuarta Enmienda, ya sea por referencia a conceptos de la ley de propiedad real o personal o entendimientos que son reconocidos y permitidos por la sociedad´. En el caso *Katz* no se redujo el ámbito de aplicación de la Cuarta Enmienda" (opinión de Scalia, adhesión de Roberts, Kennedy y Sotomayor).

"El Gobierno sostiene que varios de nuestros casos posteriores a *Katz* excluyen la conclusión de que lo que ocurrió aquí constituyó un registro. Se basa principalmente en dos casos en los que rechazamos las impugnaciones de la Cuarta Enmienda a los ´*beepers*´, dispositivos electrónicos de seguimiento que representan otra forma de vigilancia electrónica. En el primer caso, *Knotts*, rechazó la impugnación de la Cuarta Enmienda del uso de un ´*beepers*´ que se había colocado en un contenedor de cloroformo, lo que permitía a las fuerzas del orden vigilar la ubicación del contenedor. Dijimos que no se había infringido la expectativa razonable de privacidad de *Knotts*, ya que la información obtenida —la ubicación del automóvil que transportaba el contenedor en la vía pública, y la ubicación del contenedor descargado en campos abiertos cerca de la cabaña de Knotts— había sido transmitida voluntariamente al público. Pero, como ya hemos dicho, el criterio en *Katz* de expectativa razonable de intimidad se ha añadido al criterio de intrusión del *common law*, no lo ha sustituido. La sentencia en el caso *Knotts* sólo se refería al primero, ya que el segundo no estaba en cuestión. El localizador había sido colocado en el contenedor antes de que entrara en posesión de Knotts, con el consentimiento del entonces propietario. En *Knotts* no impugnó esa instalación, y nos abstuvimos específicamente de considerar su efecto en el análisis de la Cuarta Enmienda. [El caso] *Knotts* sería pertinente, tal vez, si el Gobierno argumentaba que lo que de otro modo sería un registro inconstitucional no lo es cuando sólo produce información pública. El Gobierno no presenta ese argumento, y no conocemos ningún caso que lo apoye" (opinión de Scalia, adhesión de Roberts, Kennedy y Sotomayor).

"El segundo caso ´*beeper*´, *United States v. Karo*, no sugiere una conclusión diferente. Allí abordamos la cuestión dejada abierta por *Knotts*, si la instalación de un localizador en un contenedor equivalía a un registro o una incautación. Al igual que en *Knotts*, en el momento en que se instaló el localizador, el contenedor pertenecía a un tercero, y no entró en posesión del acusado hasta más tarde. Así pues, la cuestión concreta que examinamos fue si la instalación ´con el consentimiento del propietario original constituía un registro o una incautación... cuando el contenedor se entregaba a un comprador que no tenía conocimiento de la presencia del localizador´. Sostenemos que no. El Gobierno, dijimos, entró en contacto físico con el contenedor sólo antes de que perteneciera al acusado Karo; y la transferencia del contenedor con el localizador no vigilado en su interior no transmitió ninguna información y, por lo tanto, no invadió la intimidad de Karo. Esa conclusión es perfectamente coherente con la que alcanzamos aquí. Karo aceptó el contenedor tal como le llegó, con localizador y todo, y por tanto no tenía derecho a oponerse a la presencia del localizador, aunque se utilizara para vigilar la ubicación del contenedor. Jones, que poseía el vehículo en el momento en que el Gobierno introdujo ilegalmente el dispositivo de recogida de información, se encuentra en una situación muy diferente" (opinión de Scalia, adhesión de Roberts, Kennedy y Sotomayor).

"El Gobierno también señala nuestra exposición en *New York v. Class*, en el sentido de que ´[e]l exterior de un automóvil... está a la vista del público y, por lo tanto, examinarlo no constituye un 'registro'´. Esa afirmación es de relevancia marginal aquí, ya que, como reconoce el Gobierno, ´los agentes en este caso hicieron algo más que llevar a cabo una inspección visual del vehículo del

demandado, Memorial de los Estados Unidos 41. Al fijar el dispositivo al *Jeep*, los agentes invadieron una zona protegida. Esto supondría una diferencia, ya que concluimos que el hecho de que un agente accediera momentáneamente al interior de un vehículo constituía un registro" (opinión de Scalia, adhesión de Roberts, Kennedy y Sotomayor).

"[L]a posición del Gobierno obtiene poco apoyo de nuestra conclusión en *Oliver v. United States*, en el sentido de que la intrusión de los agentes para recabar información en un ´campo abierto´ no constituía un registro en virtud de la Cuarta Enmienda, aunque fuera un allanamiento según el derecho consuetudinario. Sencillamente, un campo abierto es un lugar en el que un agente de policía no puede obtener información. Un campo abierto a diferencia del perímetro de una vivienda, véase *United States v. Dunn*, no es una de las zonas protegidas enumeradas en la Cuarta Enmienda. Ver también *Hester v. United States*. La intrusión física del Gobierno en dicha área —a diferencia de su intrusión en el ´efecto´ en cuestión aquí— no tiene importancia para la Cuarta Enmienda" (opinión de Scalia, adhesión de Roberts, Kennedy y Sotomayor).

"El Gobierno argumenta alternativamente que incluso si la colocación y el uso del dispositivo fue un registro, fue razonable —y por lo tanto legal— en virtud de la Cuarta Enmienda porque los agentes tenían sospechas razonables, y de hecho causa probable, para creer que [Jones] era un líder en una conspiración de distribución de cocaína a gran escala. No tenemos ocasión de considerar este argumento. El Gobierno no lo planteó y, por lo tanto, el Circuito de Columbia Británica no lo abordó. Consideramos que el argumento ha caducado" (opinión de Scalia, adhesión de Roberts, Kennedy y Sotomayor).

2. Derecho a la intimidad. Vigilancia electrónica. Derecho a la privacidad. Procedimiento policial. Sistema informático. Automotores. Orden judicial.

"En la era preinformática, las mayores protecciones de la intimidad no eran constitucionales ni estatutarias, sino prácticas. La vigilancia tradicional durante un periodo prolongado era difícil y costosa, por lo que rara vez se llevaba a cabo. La vigilancia de que se trata en este caso —seguimiento constante de la ubicación de un vehículo durante cuatro semanas— habría requerido un gran equipo de agentes, varios vehículos y, tal vez, asistencia aérea. Sin embargo, dispositivos como el utilizado en el presente caso hacen que la vigilancia a largo plazo sea relativamente fácil y barata. En circunstancias que implican un cambio tecnológico drástico, la mejor solución para los problemas de privacidad puede ser legislativa. Véase, por ejemplo, [el caso] *Kerr*. Un órgano legislativo está bien situado para calibrar las actitudes cambiantes del público, trazar líneas detalladas y equilibrar la privacidad y la seguridad pública de forma global" (opinión concurrente de Alito, adhesión de Ginsburg, Breyer y Kagan).

"[E]l Congreso y la mayoría de los Estados no han promulgado leyes que regulen el uso de la tecnología de localización por GPS con fines policiales. Lo mejor que podemos hacer en este caso es aplicar la doctrina existente de la Cuarta Enmienda y preguntarnos si el uso de la localización por GPS en este caso concreto supuso un grado de intrusión que una persona razonable no habría previsto" (opinión concurrente de Alito, adhesión de Ginsburg, Breyer y Kagan).

"[L]a vigilancia relativamente breve de los movimientos de una persona en la vía pública se ajusta a las expectativas de privacidad que nuestra sociedad ha reconocido como razonables. Véase *Knotts*. Pero el uso del GPS a largo plazo en las investigaciones de la mayoría de los delitos afecta a las expectativas de privacidad. En el caso de estos delitos, la sociedad espera que los agentes del orden y otras personas no vigilen en secreto y cataloguen todos y cada uno de los movimientos del vehículo de una persona durante un período muy largo, y, de hecho, en general, simplemente no pueden hacerlo. En este caso, durante cuatro semanas, los agentes del orden siguieron cada movimiento que el demandado realizaba en el vehículo que conducía. No necesitamos identificar

con precisión el punto en el que el seguimiento de este vehículo se convirtió en un registro, ya que la línea se cruzó sin duda antes de la marca de las cuatro semanas. Otros casos pueden presentar cuestiones más difíciles. Pero cuando no se sabe con certeza si un determinado período de vigilancia por GPS es lo suficientemente largo como para constituir un registro en virtud de la Cuarta Enmienda, la policía siempre puede solicitar una orden judicial. Tampoco es necesario considerar si la vigilancia prolongada por GPS en el contexto de investigaciones sobre delitos extraordinarios supondría una intromisión similar en una esfera de intimidad protegida por la Constitución. En tales casos, el seguimiento a largo plazo podría haberse llevado a cabo utilizando técnicas disponibles con anterioridad" (opinión concurrente de Alito, adhesión de Ginsburg, Breyer y Kagan).

3. Vigilancia electrónica. Automotores. Orden judicial. Consentimiento informado. Derecho a la intimidad. Razonabilidad. Protección de datos personales.

"Un registro en el sentido de la Cuarta Enmienda se produce, como mínimo, ´cuando, como aquí, el Gobierno obtiene información entrometiéndose físicamente en una zona constitucionalmente protegida´. En este caso, el Gobierno instaló un dispositivo de localización por Sistema de Posicionamiento Global (GPS) en el automóvil del demandado sin una orden válida y sin el consentimiento de su parte, y luego utilizó ese dispositivo para vigilar los movimientos del vehículo durante cuatro semanas. El Gobierno usurpó la propiedad de Jones con el fin de vigilarlo, invadiendo así los intereses de la intimidad que desde hace mucho tiempo gozan de la protección de la Cuarta Enmienda, y a la que sin duda tienen derecho. Véase, por ejemplo, *Silverman v. Estados Unidos*" (opinión concurrente de Sotomayor).

"La Cuarta Enmienda no sólo se refiere a la intrusión en la propiedad. Véase, por ejemplo, *Kyllo v. United States*. Más bien, incluso en ausencia de allanamiento, ´se produce un registro conforme a la Cuarta Enmienda cuando el gobierno viola una expectativa subjetiva de privacidad que la sociedad reconoce como razonable´, véase también *Smith v. Maryland*; *Katz v. United States* (voto concurrente de J. Harlan). En el caso *Katz*, este Tribunal amplió su enfoque hasta entonces prevaleciente sobre los derechos de propiedad al anunciar que el alcance de la Cuarta Enmienda no ´depende de la presencia o ausencia de una intrusión física´. Sin embargo, como deja claro la opinión de la mayoría, el criterio de *Katz* de expectativa razonable de privacidad aumentó, pero no desplazó ni redujo, el criterio de allanamiento del *common law* que lo precedió. Por lo tanto, ´cuando el Gobierno se involucra en la intrusión física de un área constitucionalmente protegida con el fin de obtener información, esa intrusión puede constituir una violación de la Cuarta Enmienda´. Véase *United States v. Knotts* (Brennan, J., concurrente en la sentencia); véase también, por ejemplo, *Rakas v. Illinois*" (opinión concurrente de Sotomayor).

"[P]uede ser necesario reconsiderar la premisa de que un individuo no tiene ninguna expectativa razonable de privacidad en la información revelada voluntariamente a terceros. Por ejemplo, *Smith*; *United States v. Miller*. Este enfoque se adapta mal a la era digital, en la que las personas revelan una gran cantidad de información sobre sí mismas a terceros en el curso de la realización de tareas mundanas. Las personas revelan los números de teléfono que marcan o envían a sus proveedores de telefonía móvil; las URL que visitan y las direcciones de correo electrónico con las que mantienen correspondencia a sus proveedores de servicios de Internet; y los libros, alimentos y medicamentos que compran a los minoristas en línea. Tal vez, como señala el juez Alito, algunas personas consideren que el ´intercambio´ de privacidad por comodidad ´merece la pena´, o lleguen a aceptar esta ´disminución de la privacidad´ como ´inevitable´. Por mi parte, dudo que la gente acepte sin rechistar la revelación al Gobierno, sin orden judicial, de una lista de todos los sitios web que ha visitado en la última semana, mes o año. Pero sean cuales sean las expectativas de la sociedad, sólo podrán alcanzar un estatus de protección constitucional si nuestra jurisprudencia de la Cuarta Enmienda deja de tratar el secreto como un requisito previo para la

privacidad. Yo no asumiría que toda la información revelada voluntariamente a algún miembro del público para un propósito limitado es, por esa sola razón, desprotegida por la Cuarta Enmienda. Véase [el caso] *Smith* (Marshall, J., disidente) (´La intimidad no es un bien discreto, que se posee absolutamente o no se posee en absoluto. Aquellos que revelan ciertos hechos a un banco o a una compañía telefónica para un fin comercial limitado no tienen por qué suponer que esta información se revelará a otras personas para otros fines´); véase también *Katz* (´Lo que [una persona] trata de preservar como privado, incluso en una zona accesible al público, puede estar constitucionalmente protegido´)" (opinión concurrente de Sotomayor).

2.2. CORTE SUPREMA DE JUSTICIA DE ESTADOS UNIDOS "CARPENTER V. UNITED STATES". 22/06/2018.

HECHOS

En 2011, la policía federal detuvo a cuatro hombres porque sospechaba que habían participado en el robo de algunos comercios. Posteriormente, uno de los detenidos confesó haber participado, junto con otros cómplices, en nueve robos durante los meses previos, y proporcionó al FBI los números de teléfono celular de 15 cómplices, incluyendo el número de Carpenter. En estas circunstancias, la policía le solicitó a un juez que emitiera una orden judicial con fundamento en la *Stored Communications Act* (Ley de Comunicaciones Almacenadas) para obtener datos de la ubicación del teléfono celular de Carpenter. Esta ley permite la obtención de la información de localización de teléfonos móviles (CSLI) cuando existan fundamentos razonables para creer que son relevantes y pertinentes para una investigación penal. Estas órdenes fueron emitidas por jueces federales y exigían a las compañías de telefonía celular que revelaran la información de ubicación de su teléfono durante el período de los robos. Por consiguiente, se obtuvieron 12,898 puntos de ubicación que rastreaban los movimientos de Carpenter durante cuatro meses. Luego, Carpenter fue acusado de seis cargos de robo y de portar un arma de fuego durante uno de los robos. Antes del juicio, la defensa de Carpenter solicitó que se declarara inadmisible la información de geolocalización obtenida de su teléfono celular. Para ello, argumentó que la recopilación de esa información violaba la Cuarta Enmienda por falta de una orden judicial basada en causa probable. El tribunal de primera instancia rechazó la petición. Durante el trámite del juicio, el fiscal utilizó esta misma información para establecer que el teléfono celular de Carpenter había estado en las cercanías de los cuatro lugares en los que se cometieron los robos, mientras estos ocurrían. En consecuencia, Carpenter fue declarado culpable y condenado a más de 100 años de prisión. Dicha decisión, fue apelada por su defensa. Sin embargo, el Tribunal de Apelaciones del Sexto Circuito confirmó la decisión del tribunal de grado. Para ello, el Tribunal argumentó que Carpenter no tenía una expectativa razonable de privacidad sobre la información de su ubicación obtenida por el FBI, ya que había compartido esa información con sus proveedores de servicios celulares.

DECISIÓN

La Corte Suprema de los Estados Unidos decidió, por mayoría (ministros Roberts, con la adhesión de los ministros Ginsburg, Breyer, Sotomayor y Kagan), que la adquisición de los registros de los celulares sin orden judicial por parte del gobierno constituye un registro y secuestro irrazonable en los términos de la Cuarta Enmienda.

ARGUMENTOS

1. Telefonía celular. Intervención de las telecomunicaciones. Orden judicial. Derecho a la privacidad. Derecho a la intimidad. Almacenamiento. Razonabilidad. Prueba. Prueba digital. Protección de datos personales.

"Los teléfonos móviles escanean continuamente su entorno en busca de la mejor señal, que generalmente proviene de la información de ubicación del sitio celular (CSLI) más cercano. La mayoría de los dispositivos modernos, como los teléfonos inteligentes, acceden a la red inalámbrica varias veces por minuto siempre que su señal está activada, incluso si el propietario no está utilizando una de las funciones del teléfono. Cada vez que el teléfono se conecta a una ubicación del sitio celular, genera un registro con marca de tiempo conocido como información de ubicación del sitio celular (CSLI). La precisión de esta información depende del tamaño del área geográfica cubierta por la ubicación del sitio celular. Cuanto mayor sea la concentración de

ubicaciones de los sitios celulares, menor será el área de cobertura. A medida que ha aumentado el uso de datos de los teléfonos celulares, los proveedores de servicios inalámbricos han instalado más ubicaciones de los sitios celulares para manejar el tráfico. Esto ha llevado a áreas de cobertura cada vez más compactas, especialmente en las zonas urbanas" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Los proveedores de servicios inalámbricos recopilan y almacenan CSLI para sus propios fines comerciales, incluida la búsqueda de puntos débiles en su red y la aplicación de cargos de ´*roaming*´ cuando otro proveedor enruta datos a través de sus ubicaciones de los sitios celulares. Además, los proveedores de servicios inalámbricos a menudo venden registros de ubicación agregados a intermediarios de datos, sin información de identificación individual del tipo que se discute aquí. Si bien los operadores han retenido durante mucho tiempo CSLI para el inicio y el final de las llamadas entrantes, en los últimos años las compañías telefónicas también han recopilado información de ubicación a partir de la transmisión de mensajes de texto y conexiones de datos de rutina. En consecuencia, los teléfonos móviles modernos generan cantidades cada vez mayores de CSLI cada vez más precisos" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"La Cuarta Enmienda protege ´el derecho de las personas a estar seguros en sus personas, casas, papeles y efectos, contra registros y secuestros irrazonables´. El ´propósito básico de esta Enmienda´, ´es salvaguardar la privacidad y seguridad de las personas contra invasiones arbitrarias por parte de funcionarios gubernamentales´" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"[L]a Corte ha reconocido que ´los derechos de propiedad no son la única medida de las violaciones de la Cuarta Enmienda´. Ver *Soldal v. el condado de Cook.* En el caso *Katz v. United States*, establecimos que ´la Cuarta Enmienda protege a las personas, no a los lugares´ y ampliamos nuestra concepción de la Enmienda para proteger también ciertas expectativas de privacidad. Cuando un individuo ´busca preservar algo como privado´ y su expectativa de privacidad es ´una que la sociedad está dispuesta a reconocer como razonable´, hemos sostenido que la intrusión oficial en esa esfera privada generalmente califica como un registro y requiere una orden judicial respaldada por una causa probable. Ver el caso *Smith*" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Aunque ninguna rúbrica resuelve definitivamente qué expectativas de privacidad tienen derecho a protección, el análisis se basa en interpretaciones históricas ´de lo que se consideró un registro y secuestro irrazonables cuando se adoptó [la Cuarta Enmienda]´. Ver *Carroll v. Estados Unidos.* En este sentido, nuestros casos han reconocido algunas pautas básicas. Primero, que la Enmienda busca proteger ´la privacidad de la vida´ contra el ´poder arbitrario´. Ver *Boyd v. Estados Unidos.* En segundo lugar, y de manera relacionada, que un objetivo central de los redactores [de la constitución] era ´colocar obstáculos en el camino de una vigilancia policial demasiado penetrante´. Ver *Estados Unidos v. Di Re*" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Hemos tenido presente esta atención a los entendimientos de la época de los fundadores al aplicar la Cuarta Enmienda a las innovaciones en herramientas de vigilancia. A medida que la tecnología ha mejorado la capacidad del Gobierno para invadir áreas normalmente protegidas de miradas inquisitivas, este Tribunal ha buscado ´asegurar la preservación de ese grado de privacidad frente al gobierno que existía cuando se adoptó la Cuarta Enmienda´. Ver *Kyllo v. Estados Unidos*. Por esa razón, rechazamos en el caso *Kyllo* una ´interpretación mecánica´ de la Cuarta Enmienda y sostuvimos que el uso de una cámara termográfica para detectar el calor que irradia desde el costado de la casa del acusado era un registro. Debido a que cualquier otra

conclusión dejaría a los propietarios de viviendas ´a merced del avance de la tecnología´, determinamos que el Gobierno, a falta de una orden judicial, no podía aprovechar esa nueva tecnología que mejora los sentidos para explorar lo que estaba sucediendo dentro del hogar" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Asimismo, en *Riley*, el Tribunal reconoció la ´inmensa capacidad de almacenamiento´ de los teléfonos celulares modernos al sostener que los agentes de policía generalmente deben obtener una orden judicial antes de registrar el contenido de un teléfono. Explicamos que si bien la regla general que permite registros sin orden judicial para arrestos ´logra el equilibrio apropiado en el contexto de objetos físicos, ninguno de sus fundamentos tiene mucha fuerza con respecto ´al vasto almacén de información confidencial en un teléfono celular'" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"El caso que tenemos ante nosotros involucra la adquisición por parte del Gobierno de registros de ubicaciones de los sitios celulares de operadores inalámbricos que revelan la ubicación del teléfono celular de Carpenter cada vez que hacía o recibía llamadas. Este tipo de datos digitales (información de ubicación personal mantenida por un tercero) no encaja perfectamente en los precedentes existentes. En cambio, las solicitudes de registros de ubicaciones de los sitios celulares se encuentran en la intersección de dos líneas de casos, los cuales informan nuestra comprensión de los intereses de privacidad en juego" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"El primer conjunto de casos aborda la expectativa de privacidad de una persona en cuanto a su ubicación física y sus movimientos. En *Estados Unidos v. Knotts*, consideramos el uso por parte del Gobierno de un ´*beeper*´ para ayudar a rastrear un vehículo a través del tráfico. En ese caso, los agentes de policía colocaron un '*beeper*' en un contenedor de cloroformo antes de que uno de los cómplices de Knotts lo comprara. Luego, los oficiales (con asistencia aérea intermitente) siguieron el automóvil que transportaba el contenedor desde Minneapolis hasta la cabaña de Knotts en Wisconsin, confiando en la señal del '*beeper*' para ayudar a mantener el vehículo a la vista. La Corte concluyó que la vigilancia visual ´aumentada´ no constituía un registro porque ´una persona que viaja en un automóvil por la vía pública no tiene expectativas razonables de privacidad en sus movimientos de un lugar a otro´. Dado que los movimientos del vehículo y su destino final habían sido ´transmitidos voluntariamente a cualquiera que quisiera verlo´, no podía afirmar un interés de privacidad en la información obtenida" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"[E]ste Tribunal en *Knotts* tuvo cuidado de distinguir entre el rastreo rudimentario facilitado por el '*beeper*' y modos de vigilancia más amplios. El Tribunal enfatizó el ´uso limitado que el gobierno hizo de las señales de este '*beeper*' en particular´ durante un ´viaje automotor´. Significativamente, la Corte se reservó la pregunta de si ´diferentes principios constitucionales podrían ser aplicables´ si ´fuese posible la vigilancia las veinticuatro horas de cualquier ciudadano de este país´" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Tres décadas más tarde, la Corte consideró una vigilancia más sofisticada como la prevista en el caso *Knotts* y concluyó que efectivamente se aplicaban principios diferentes. En *Estados Unidos v. Jones*, los agentes del FBI instalaron un dispositivo de rastreo GPS en el vehículo de Jones y monitorearon remotamente los movimientos del vehículo durante 28 días. El Tribunal decidió el caso basándose en la invasión física del vehículo por parte del Gobierno. Al mismo tiempo, cinco jueces coincidieron en que se plantearían preocupaciones relacionadas con la privacidad, por ejemplo, ´activando subrepticiamente un sistema de detección de vehículos robados´ en el automóvil de Jones para rastrear al propio Jones, o realizando un rastreo por GPS de su teléfono

celular. Dado que el monitoreo por GPS de un vehículo rastrea ´cada movimiento´ que una persona hace en ese vehículo, los jueces concurrentes concluyeron que ´el monitoreo por GPS a más largo plazo en las investigaciones de la mayoría de los delitos afecta las expectativas de privacidad´, independientemente de si esos movimientos fueron revelados al público en grande" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"En una segunda serie de decisiones, el Tribunal ha trazado una línea entre lo que una persona guarda para sí y lo que comparte con los demás. Anteriormente hemos sostenido que ´una persona no tiene expectativas legítimas de privacidad en la información que entrega voluntariamente a terceros´. Esto sigue siendo cierto ´incluso si la información se revela bajo el supuesto de que se utilizará sólo para un propósito limitado´. Ver *Estados Unidos v Miller*. Como resultado, el gobierno suele ser libre de obtener dicha información del destinatario sin activar las protecciones de la Cuarta Enmienda" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Esta doctrina de terceros tiene sus raíces en gran medida en [el caso] *Miller*. Mientras investigaba a Miller por evasión fiscal, el gobierno citó a sus bancos, exigiendo varios meses de cheques cancelados, comprobantes de depósito y extractos mensuales. El Tribunal rechazó una impugnación de la Cuarta Enmienda a la recopilación de registros. Por un lado, Miller no podía ´afirmar ni la propiedad ni la posesión´ de los documentos; eran ´registros comerciales de los bancos. Por otro lado, la naturaleza de esos registros confirmó la expectativa limitada de privacidad de Miller, porque los cheques ´no eran comunicaciones confidenciales sino instrumentos negociables para ser utilizados en transacciones comerciales´, y los extractos bancarios contenían información ´expuesta a empleados en el curso ordinario de sus negocios´. Por lo tanto, el Tribunal concluyó que Miller había ´asumido el riesgo, al revelar sus asuntos a otra persona, de que la información [sería] transmitida por esa persona al Gobierno´" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Tres años más tarde, en [el caso] *Smith* se aplicó los mismos principios en el contexto de la información transmitida a una compañía telefónica. El Tribunal dictaminó que el uso por parte del Gobierno de un lápiz registrador (un dispositivo que registraba los números de teléfono salientes marcados en un teléfono fijo) no era un registro. Al señalar las ´capacidades limitadas´ del registro de lápiz, el Tribunal ´dudó de que las personas en general tengan alguna expectativa real de privacidad en los números que marcan´. Los suscriptores de telefonía saben, después de todo, que la compañía telefónica utiliza los números ´para una variedad de propósitos comerciales legítimos´, incluido el enrutamiento de llamadas. Y, en cualquier caso, explicó la Corte, tal expectativa ´no es algo que la sociedad esté dispuesta a reconocer como razonable´. Cuando Smith realizó una llamada, ´transmitió voluntariamente´ los números marcados a la compañía telefónica ´exponiendo esa información a su equipo en el curso normal de sus negocios´. Una vez más, sostuvimos que el acusado ´asumió el riesgo´ de que los registros de la empresa ´serían divulgados a la policía´" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"La pregunta que enfrentamos hoy es cómo aplicar la Cuarta Enmienda a un nuevo fenómeno: la capacidad de registrar los movimientos pasados de una persona a través del registro de las señales de su teléfono celular. Este seguimiento comparte muchas de las cualidades del seguimiento por GPS que consideramos en Jones. Al igual que el rastreo por GPS de un vehículo, la información de ubicación del teléfono celular es detallada, enciclopédica y se compila sin esfuerzo" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Al mismo tiempo, el hecho de que el individuo revele continuamente su ubicación a su proveedor de servicios inalámbricos implica el principio de terceros de los casos *Smith* y *Miller*. Pero si bien

la doctrina del tercero se aplica a números de teléfono y registros bancarios, no está claro si su lógica se extiende a la categoría cualitativamente diferente de registros de ubicaciones de los sitios celulares. Después de todo, cuando se decidió por *Smith* en 1979, pocos podrían haber imaginado una sociedad en la que un teléfono vaya a donde quiera que vaya su propietario, transmitiendo al proveedor de servicios inalámbricos no sólo los dígitos marcados, sino un registro detallado y completo de los movimientos de la persona" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Nos negamos a extender *Smith* y *Miller* para cubrir estas circunstancias novedosas. Dada la naturaleza única de los registros de ubicación de teléfonos celulares, el hecho de que la información esté en manos de un tercero no supera por sí solo el reclamo del usuario de protección de la Cuarta Enmienda. Ya sea que el gobierno emplee su propia tecnología de vigilancia como en *Jones* o aproveche la tecnología de un proveedor de servicios inalámbricos, sostenemos que un individuo mantiene una expectativa legítima de privacidad en el registro de sus movimientos físicos capturados a través de CSLI. La información de ubicación obtenida de los proveedores de servicios inalámbricos de Carpenter fue producto de un registro" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Una persona no renuncia a toda la protección de la Cuarta Enmienda al aventurarse en la esfera pública. Por el contrario, ´lo que uno busca preservar como privado, incluso en un área accesible al público, puede estar protegido constitucionalmente´. Ver *Katz.* Una mayoría de este Tribunal ya ha reconocido que los individuos tienen una expectativa razonable de privacidad en el conjunto de sus movimientos físicos. Ver el caso *Jones*. Antes de la era digital, las fuerzas del orden podían haber perseguido a un sospechoso durante un breve período, pero hacerlo ´durante un período prolongado era difícil y costoso y, por lo tanto, rara vez se llevaba a cabo´. Por esa razón, ´la expectativa de la sociedad ha sido que los agentes encargados de hacer cumplir la ley y otros no monitorearían y catalogarían en secreto cada movimiento del automóvil de un individuo durante un período muy largo (y, de hecho, en general, simplemente no podrían)´" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Permitir el acceso del gobierno a los registros de las instalaciones celulares contraviene esa expectativa. Aunque dichos registros se generan con fines comerciales, esa distinción no niega la anticipación de Carpenter sobre la privacidad en su ubicación física. Mapear la ubicación de un teléfono celular a lo largo de 127 días proporciona un registro completo del paradero de su titular. Al igual que con la información del GPS, los datos con marca de tiempo proporcionan una ventana íntima a la vida de una persona, revelando no sólo sus movimientos particulares, sino a través de ellos sus ´asociaciones familiares, políticas, profesionales, religiosas y sexuales´. Estos registros de ubicación contienen para muchos estadounidenses las 'privacidades de la vida'. Y al igual que el monitoreo por GPS, el rastreo de teléfonos celulares es notablemente fácil, económico y eficiente en comparación con las herramientas de investigación tradicionales. Con solo hacer clic en un botón, el Gobierno puede acceder al profundo repositorio de información de ubicación histórica de cada operador prácticamente sin costo alguno" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"[L]os registros históricos de las ubicaciones de los sitios celulares presentan preocupaciones de privacidad aún mayores que el monitoreo por GPS de un vehículo que consideramos en Jones. A diferencia del contenedor con micrófonos en *Knotts* o el auto en *Jones*, un teléfono celular —casi una ´característica de la anatomía humana´— rastrea casi exactamente los movimientos de su dueño. Si bien las personas salen regularmente de sus vehículos, llevan consigo de manera compulsiva sus teléfonos celulares todo el tiempo. Un teléfono celular sigue fielmente a su dueño más allá de las vías públicas y hasta residencias privadas, consultorios médicos, sedes políticas y otros lugares potencialmente reveladores. En consecuencia, cuando el Gobierno rastrea la

ubicación de un teléfono celular logra una vigilancia casi perfecta, como si hubiera colocado un monitor en el tobillo del usuario del teléfono" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"[L]a calidad retrospectiva de los datos aquí brinda a la policía acceso a una categoría de información que de otro modo sería incognoscible. En el pasado, los intentos de reconstruir los movimientos de una persona están limitados por la escasez de registros y la debilidad de la memoria. Con acceso a CSLI, el Gobierno ahora puede viajar en el tiempo para rastrear el paradero de una persona, sujeto únicamente a las políticas de retención de los proveedores de servicios inalámbricos, que actualmente mantienen registros por hasta cinco años. Fundamentalmente, debido a que la información de ubicación se registra continuamente para los 400 millones de dispositivos en los Estados Unidos (no sólo los que pertenecen a personas que podrían ser objeto de investigación), esta nueva capacidad de seguimiento va en contra de todos. A diferencia del dispositivo GPS de Jones, la policía ni siquiera necesita saber de antemano si quiere seguir a una persona concreta ni cuándo" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Quienquiera que sea el sospechoso, efectivamente ha sido seguido en todo momento de cada día durante cinco años, y la policía puede (en opinión del Gobierno) invocar los resultados de esa vigilancia sin tener en cuenta las limitaciones de la Cuarta Enmienda. Sólo los pocos que no tenían teléfonos móviles podían escapar de esta vigilancia incansable y absoluta" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"[E]l Gobierno y el Juez Kennedy sostienen que debería permitirse la recopilación de CSLI porque los datos son menos precisos que la información del GPS. No hay que preocuparse, sostienen, porque los registros de ubicación ´no fueron suficientes por sí solos para ubicar a [Carpenter] en la escena del crimen´; lo ubicaron dentro de un sector en forma de cuña que abarcaba desde un octavo hasta cuatro millas cuadradas. Sin embargo, la Corte ya ha rechazado la proposición de que ´la inferencia aísla un registro´. A partir de los 127 días de datos de ubicación que recibió, el Gobierno pudo, en combinación con otra información, deducir un registro detallado de los movimientos de Carpenter, incluso cuando estuvo en el lugar de los robos. Y el Gobierno consideró que el CSLI era lo suficientemente acertado como para destacar durante el alegato final de su juicio" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"[L]a norma que adopte la Corte ´debe tener en cuenta sistemas más sofisticados que ya están en uso o en desarrollo´. Si bien los registros en este caso reflejan el estado de la tecnología a principios de la década, la precisión del CSLI se está acercando rápidamente a la precisión del nivel del GPS. A medida que ha proliferado el número de ubicaciones de los sitios celulares, el área geográfica cubierta por cada sector celular se ha reducido, particularmente en las áreas urbanas. Además, con la nueva tecnología que mide el tiempo y el ángulo de las señales que llegan a sus torres, los proveedores de servicios inalámbricos ya tienen la capacidad de localizar la ubicación de un teléfono dentro de un radio de 50 metros" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"[C]uando el Gobierno accedió a CSLI desde los proveedores de servicios inalámbricos, invadió la expectativa razonable de privacidad de Carpenter en todos sus movimientos físicos" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"El principal argumento contrario del Gobierno es que la doctrina del tercero rige este caso. En su opinión, los registros de las ubicaciones de los sitios celulares son un juego limpio porque son 'registros comerciales' creados y mantenidos por los proveedores de servicios inalámbricos. El

Gobierno (junto con el Juez Kennedy) reconoce que este caso presenta nueva tecnología, pero afirma que, no obstante, la cuestión legal gira en torno a una solicitud común de información por parte de un tercer testigo" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"La posición del Gobierno no logra enfrentar los cambios sísmicos en la tecnología digital que hicieron posible el seguimiento no sólo de la ubicación de Carpenter sino también de la de todos los demás, no por un período corto sino durante años y años. Sprint Corporation y sus competidores no son los típicos testigos. A diferencia del vecino entrometido que vigila las idas y venidas, ellos están siempre alerta y su memoria es casi infalible. Hay una gran diferencia entre los tipos limitados de información personal abordados en *Smith* y *Miller* y la crónica exhaustiva de la información de ubicación recopilada casualmente por los proveedores de servicios inalámbricos en la actualidad. Por lo tanto, el Gobierno no pide una aplicación directa de la doctrina del tercero, sino más bien una extensión significativa de ella a una categoría distinta de información" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"La doctrina del tercero surge en parte de la noción de que un individuo tiene una expectativa reducida de privacidad en la información que comparte conscientemente con otro. Pero el hecho de que ´los intereses de privacidad hayan disminuido no significa que la Cuarta Enmienda quede completamente fuera de escena´. Después de todo, no se basaron únicamente en el acto de compartir. En cambio, consideraron ´la naturaleza de los documentos particulares buscados´ para determinar si ´existe una 'expectativa de privacidad' legítima con respecto a su contenido´. En el caso *Smith* señaló las capacidades limitadas de un registro de pluma; como se explica en Riley, los registros de llamadas telefónicas revelan poco en cuanto a ´información de identificación´. En el caso *Miller* también se señaló que los cheques ´no eran comunicaciones confidenciales sino instrumentos negociables para ser utilizados en transacciones comerciales´. Al aplicar mecánicamente la doctrina del tercero a este caso, el Gobierno no aprecia que no existen limitaciones comparables a la naturaleza reveladora del CSLI" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"De hecho, la Corte ya ha mostrado especial atención a la información sobre la localización en el contexto de terceros. En *Knotts*, el Tribunal se basó en *Smith* para sostener que un individuo no tiene expectativas razonables de privacidad en los movimientos públicos que ´transmitió voluntariamente a cualquiera que quisiera mirar´. Pero cuando se enfrentaron a un seguimiento más generalizado, cinco jueces coincidieron en que el seguimiento por GPS a largo plazo de incluso un vehículo que circula por la vía pública constituye un registro. El juez Gorsuch se pregunta por qué ´la ubicación de alguien cuando usa un teléfono´ es sensible, y el Juez Kennedy supone que los movimientos discretos de una persona ´no son particularmente privados´. Sin embargo, este caso no se trata de ´usar un teléfono´ o el movimiento de una persona en un momento determinado. Se trata de una crónica detallada de la presencia física de una persona recopilada cada día, cada momento, durante varios años. Una crónica de este tipo implica preocupaciones sobre la privacidad mucho más allá de las consideradas en *Smith* y *Miller*" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Tampoco se sostiene el segundo fundamento subyacente a la doctrina del tercero (la exposición voluntaria) cuando se trata de CSLI. La información de ubicación del teléfono celular no se ´comparte´ en realidad como normalmente se entiende el término. En primer lugar, los teléfonos celulares y los servicios que brindan son ´una parte tan omnipresente e insistente de la vida diaria´ que llevarlos consigo es indispensable para participar en la sociedad moderna. En segundo lugar, un teléfono móvil registra un registro de sitio móvil gracias a su funcionamiento, sin ningún acto afirmativo por parte del usuario más allá del encendido. Prácticamente cualquier actividad en el teléfono genera CSLI, incluidas llamadas entrantes, mensajes de texto o correos electrónicos e

innumerables otras conexiones de datos que un teléfono realiza automáticamente cuando busca noticias, clima o actualizaciones de redes sociales. Aparte de desconectar el teléfono de la red, no hay forma de evitar dejar un rastro de datos de ubicación. Como resultado, en ningún sentido significativo el usuario ´asume voluntariamente el riesgo´ de entregar un expediente completo de sus movimientos físicos" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"[N]os negamos a extender *Smith* y *Miller* a la colección de CSLI. Dada la naturaleza única de la información de ubicación de teléfonos celulares, el hecho de que el Gobierno haya obtenido la información de un tercero no supera el reclamo de Carpenter de protección de la Cuarta Enmienda. La adquisición por parte del Gobierno de los registros de las instalaciones celulares fue un registro en el sentido de la Cuarta Enmienda" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Nuestra decisión de hoy es limitada. No expresamos una opinión sobre asuntos que no tenemos ante nosotros: CSLI en tiempo real o ´volcados de torre´ (una descarga de información en todos los dispositivos que se conectaron a una ubicación del sitio celular en particular durante un intervalo particular). No perturbamos la aplicación de los precedentes *Smith* y *Miller* ni cuestionamos las técnicas y herramientas de vigilancia convencionales, como las cámaras de seguridad. Tampoco abordamos otros registros comerciales que accidentalmente podrían revelar información de ubicación. Además, nuestra opinión no considera otras técnicas de recopilación que involucren asuntos exteriores o seguridad nacional. Como señaló el juez Frankfurter al considerar nuevas innovaciones en aviones y radios, la Corte debe actuar con cuidado en tales casos, para garantizar que no ´avergoncemos al futuro´" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Habiendo descubierto que la adquisición del CSLI de Carpenter fue un registro, también concluimos que el Gobierno generalmente debe obtener una orden respaldada por una causa probable antes de adquirir dichos registros. Aunque la ´medida última de la constitucionalidad de una búsqueda gubernamental es la 'razonabilidad'´, nuestros casos establecen que los registros sin orden judicial generalmente no son razonables cuando ´funcionarios encargados de hacer cumplir la ley llevan a cabo un registro para descubrir evidencia de irregularidades criminales´. Por lo tanto, ´en ausencia de una orden judicial, un registro es razonable sólo si cae dentro de una excepción específica al requisito de la orden judicial´" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"El Gobierno adquirió los registros de las instalaciones celulares de conformidad con una orden judicial emitida en virtud de la Ley de Comunicaciones Almacenadas, que exigía que el Gobierno mostrara ´motivos razonables´ para creer que los registros eran ´relevantes y sustanciales para una investigación en curso´. Esa demostración está muy por debajo de la causa probable requerida para una orden judicial. El Tribunal suele exigir ´alguna cantidad de sospecha individualizada´ antes de que pueda llevarse a cabo un registro o secuestro. Sin embargo, según la norma de la Ley de Comunicaciones Almacenadas, las fuerzas del orden sólo necesitan demostrar que la evidencia de la ubicación del sitio celular podría ser pertinente para una investigación en curso, una desviación ´gigantesca´ de la regla de causa probable, como el Gobierno explica más adelante. En consecuencia, una orden emitida bajo la Sección 2703(d) de la Ley no es un mecanismo permisible para acceder a registros históricos de ubicaciones de los sitios celulares. Antes de obligar a un proveedor de servicios inalámbricos a entregar el CSLI de un suscriptor, la obligación del gobierno es familiar: obtener una orden judicial" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

“El Juez Alito sostiene que el requisito de la orden judicial simplemente no se aplica cuando el Gobierno adquiere registros mediante un proceso obligatorio. A diferencia de un registro real, dice, las citaciones para la obtención de documentos no implican la obtención directa de pruebas; son, como mucho, un ´registro constructivo´ realizada por el destinatario de la citación. Dada esta menor intrusión en la privacidad personal, el Juez Alito sostiene que la producción obligatoria de registros no se rige por el mismo estándar de causa probable. En su opinión, los precedentes de esta Corte establecen una regla categórica, separada y distinta de la doctrina del tercero, que somete las citaciones a un escrutinio indulgente sin tener en cuenta la expectativa de privacidad de los registros del sospechoso” (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

“Pero este Tribunal nunca ha sostenido que el Gobierno pueda citar a terceros para que presenten registros en los que el sospechoso tenga una expectativa razonable de privacidad. Casi todos los ejemplos que cita el Juez Alito, contemplaban solicitudes de pruebas que implicaran una disminución de los intereses de privacidad o de los propios libros de una corporación. La única excepción, por supuesto, es el precedente *Miller*, donde el análisis de la Corte de la citación del tercero se fusionó con la aplicación de la doctrina del tercero” (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

“El Juez Alito pasa por alto la cuestión crítica. En algún momento, los disidentes deberían reconocer que el CSLI es un tipo de registro empresarial completamente diferente, algo que implica preocupaciones básicas de la Cuarta Enmienda sobre el poder arbitrario del gobierno de manera mucho más directa que los impuestos corporativos o los libros de nómina. Al enfrentar nuevas preocupaciones generadas por la tecnología digital, esta Corte ha tenido cuidado de no extender acríticamente los precedentes existentes” (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

“Si la opción de proceder mediante citación proporcionara una limitación categórica a la protección de la Cuarta Enmienda, ningún tipo de registro estaría jamás protegido por el requisito de la orden judicial. Según la opinión del Juez Alito, las cartas privadas, el contenido digital de un teléfono celular (cualquier información personal reducida a forma de documento, de hecho) pueden recopilarse mediante citación judicial sin otro motivo que la ´curiosidad oficial´. El Juez Kennedy se niega a adoptar las implicaciones radicales de esta teoría, dejando abierta la cuestión de si el requisito de la orden judicial se aplica ´cuando el gobierno obtiene los equivalentes modernos de los 'documentos' o 'efectos' propios de un individuo, incluso cuando esos documentos o efectos son en poder de un tercero´. Sería una excepción sensata, porque impediría que la doctrina de la citación supere cualquier expectativa razonable de privacidad. Si la doctrina del tercero no se aplica a los ´equivalentes modernos de los 'papeles' o 'efectos' propios de un individuo´, entonces la implicación clara es que los documentos deberían recibir plena protección de la Cuarta Enmienda. Simplemente pensamos que dicha protección debería extenderse también a un registro detallado de los movimientos de una persona durante varios años” (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

“Ciertamente, esto no quiere decir que todas las órdenes que obliguen a la presentación de documentos requieran una demostración de causa probable. El Gobierno podrá utilizar citaciones para adquirir registros en la inmensa mayoría de las investigaciones. Solo sostenemos que se requiere una orden judicial en el raro caso en que el sospechoso tenga un interés legítimo de privacidad en los registros en poder de un tercero” (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

“[A]unque el Gobierno generalmente necesitará una orden judicial para acceder al CSLI, las excepciones de casos específicos pueden respaldar una búsqueda sin orden judicial de los

registros de las ubicaciones de los sitios celulares de un individuo bajo ciertas circunstancias. ´Una excepción bien reconocida se aplica cuando 'las exigencias de la situación hacen que las necesidades de aplicación de la ley sean tan apremiantes que un registro sin orden judicial es objetivamente razonable según la Cuarta Enmienda´. Tales exigencias incluyen la necesidad de perseguir a un sospechoso que huye, proteger a las personas que están amenazadas de daño inminente o evitar la destrucción inminente de pruebas" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"[S]i las fuerzas del orden se enfrentan a una situación urgente, tales amenazas específicas probablemente justificarán la recolección sin orden judicial de CSLI. Los tribunales inferiores, por ejemplo, han aprobado registros sin orden judicial relacionados con amenazas de bomba, tiroteos activos y secuestros de niños. Nuestra decisión de hoy no pone en duda el acceso sin orden judicial a CSLI en tales circunstancias. Si bien la policía debe obtener una orden judicial al recolectar CSLI para ayudar en la investigación criminal de casos comunes, la regla que establecimos no limita su capacidad para responder a una emergencia en curso" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Como explicó el juez Brandeis en su famosa disidencia, la Corte está obligada —a medida que ´el Gobierno dispone de medios más sutiles y de mayor alcance para invadir la privacidad´— a garantizar que el ´progreso de la ciencia´ no erosione la protección de la Cuarta Enmienda. Aquí el progreso de la ciencia ha brindado a las fuerzas del orden una nueva y poderosa herramienta para llevar a cabo sus importantes responsabilidades. Al mismo tiempo, esta herramienta corre el riesgo de una invasión gubernamental del tipo que los redactores, ´después de consultar las lecciones de la historia´, redactaron la Cuarta Enmienda para prevenir" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

"Nos negamos a otorgar al estado acceso sin restricciones a la base de datos de información de ubicación física de un proveedor de servicios inalámbricos. A la luz de la naturaleza profundamente reveladora de CSLI, su profundidad, amplitud y alcance integral, y la naturaleza ineludible y automática de su recopilación, el hecho de que dicha información sea recopilada por un tercero no la hace menos merecedora de la protección de la Cuarta Enmienda. La adquisición por parte del Gobierno de los registros de las ubicaciones de los sitios celulares aquí fue un registro bajo esa Enmienda" (opinión del juez Robert, adhesión de los jueces Ginsburg, Breyer, Sotomayor y Kagan).

2.3. TRIBUNAL EUROPEO DE DERECHOS HUMANOS, GRAN SALA, "ROMAN ZAKHAROV V. RUSIA". CASO N° 47143/06. 4/12/2015.

HECHOS

En diciembre de 2003, un editor jefe de una editorial y revista de aviación, quien también presidía una ONG dedicada a monitorear la libertad de los medios en Rusia, inició un proceso judicial contra tres operadores de telefonía móvil ante el Tribunal de Distrito de Vasileostrovskiy de San Petersburgo. El demandante argumentó que, en cumplimiento de la Orden No. 70 del Comité Estatal de Comunicaciones e Informática, los operadores habían instalado equipos que permitían al Servicio Federal de Seguridad (FSB) interceptar todas las comunicaciones telefónicas sin autorización judicial previa. Además, sostuvo que esta orden, que nunca había sido publicada oficialmente, restringía indebidamente su derecho a la privacidad. Dos años después, en diciembre de 2005, el Tribunal de Distrito desestimó las pretensiones del demandante, considerando que no había demostrado que los operadores hubieran transmitido información protegida a personas no autorizadas. Ante esta decisión, el demandante interpuso un recurso de apelación. No obstante, en abril de 2006, el Tribunal de la Ciudad de San Petersburgo confirmó la sentencia inicial. Frente a esta decisión, el demandante realizó la presentación ante el Tribunal Europeo de Derechos Humanos. Para ello, sostuvo que el sistema de vigilancia secreta de comunicaciones móviles en Rusia violaba su derecho al respeto de su vida privada y correspondencia. Para fundamentar su postura, argumentó que la legislación rusa permitía la interceptación generalizada de comunicaciones móviles sin salvaguardias adecuadas contra abusos, no definía claramente las circunstancias para la vigilancia secreta, ni establecía límites sobre su duración. Asimismo, cuestionó los procedimientos para manejar los datos interceptados y criticó la falta de supervisión efectiva y de notificación a los sujetos de vigilancia. Por su parte, el Gobierno ruso presentó una doble defensa. En primer lugar, argumentó que el demandante no podía reclamar ser víctima de una violación de sus derechos, ya que no había demostrado que sus comunicaciones hubieran sido interceptadas. En segundo lugar, sostuvo que existían recursos efectivos disponibles en la legislación rusa que el demandante no había agotado.

DECISIÓN

La Gran Sala del Tribunal Europeo de Derechos Humanos consideró que Rusia era responsable por la violación del derecho al respeto de la vida privada y la correspondencia (artículo 8 del Convenio Europeo de Derechos Humanos).

ARGUMENTOS

1. Derecho a la privacidad. Principio de legalidad. Vigilancia electrónica. Democracia.

"El Tribunal reitera que cualquier injerencia sólo puede justificarse en virtud del artículo 8 apartado 2 si es conforme a Derecho, persigue uno o varios de los fines legítimos a los que se refiere ese apartado y es necesaria en una sociedad democrática para alcanzar cualquiera de dichos fines (véase la sentencia *Kennedy*)" (párrafo 227).

"El Tribunal ha sostenido en varias ocasiones que la referencia a la ´previsibilidad´ en el contexto de la interceptación de las comunicaciones no puede ser la misma que en muchos otros ámbitos. La previsibilidad en el contexto especial de las medidas secretas de vigilancia, como la interceptación de las comunicaciones, no puede significar que un individuo deba poder prever cuándo es probable que las autoridades intercepten sus comunicaciones para poder adaptar su conducta. Sin embargo, especialmente cuando un poder conferido al ejecutivo se ejerce en secreto, los riesgos de arbitrariedad son evidentes. Por lo tanto, es esencial disponer de normas claras y detalladas sobre la interceptación de las conversaciones telefónicas, sobre todo porque la tecnología disponible para su uso es cada vez más sofisticada. La legislación nacional debe ser lo suficientemente clara como para dar a los ciudadanos una indicación adecuada de las

circunstancias y condiciones en que las autoridades están facultadas para recurrir a tales medidas (véase *Malone*; *Leander v. Suecia*; *Huvig v. Francia*; *Valenzuela Contreras v. España*; *Rotaru*; *Weber y Saravia*; y *Asociación para la Integración Europea y los Derechos Humanos* y *Ekimdzhiev*)" (párrafo 229).

"[L]a legalidad de la injerencia está estrechamente relacionada con la cuestión de si se ha cumplido el criterio de "necesidad" y, por lo tanto, es apropiado que el Tribunal aborde conjuntamente los requisitos de ´conformidad con la ley´ y de ´necesidad´ (véase *Kennedy*; véase también *Kvasnica*). La ´calidad de la ley´ en este sentido implica que la legislación nacional no sólo debe ser accesible y previsible en su aplicación, sino que también debe garantizar que las medidas de vigilancia secreta sólo se apliquen cuando sean ´necesarias en una sociedad democrática´, en particular, estableciendo salvaguardias y garantías adecuadas y efectivas contra los abusos" (párrafo 236).

"Las partes no han discutido que las interceptaciones de las comunicaciones telefónicas móviles tienen un fundamento en el derecho interno. Se rigen, en particular, por el CCrP [*Code of Criminal Procedure*] y la OSAA [*Operational Search Activities Act*], así como por la Ley de Comunicaciones y las Órdenes emitidas por el Ministerio de Comunicaciones. Además, el Tribunal considera evidente que las medidas de vigilancia permitidas por la legislación rusa persiguen los objetivos legítimos de protección de la seguridad nacional y de la seguridad pública, de prevención de la delincuencia y de protección del bienestar económico del país. Por tanto, queda por determinar si la legislación rusa es accesible y contiene salvaguardias y garantías adecuadas y efectivas para cumplir los requisitos de ´previsibilidad´ y ´necesidad en una sociedad democrática´ (párrafo 237).

2. Derecho a la información. Publicidad. Reglamentos de los derechos. Acceso a la justicia.

"La publicación de la Orden en la revista oficial *SvyazInform* del Ministerio de Comunicaciones, distribuida mediante suscripción, la puso a disposición únicamente de los especialistas en comunicaciones y no del público en general. Al mismo tiempo, el Tribunal observa que se puede acceder al texto de la Orden, con los anexos, a través de una base de datos jurídica en línea de mantenimiento privado, que lo reprodujo a partir de la publicación en *SvyazInform*. El Tribunal considera lamentable la falta de una publicación oficial de acceso general de la Orden no. 70. Sin embargo, teniendo en cuenta el hecho de que ha sido publicada en una revista ministerial oficial, junto con el hecho de que puede ser consultada por el público en general a través de una base de datos jurídica en línea, el Tribunal no considera necesario profundizar en la cuestión de la accesibilidad de la ley nacional. En su lugar, se concentrará en los requisitos de ´previsibilidad´ y de ´necesidad´" (párrafo 242).

3. Control judicial. Vigilancia electrónica. Principio de proporcionalidad.

"El Tribunal recuerda que la legislación nacional debe definir el ámbito de aplicación de las medidas de vigilancia secreta indicando adecuadamente a los ciudadanos las circunstancias en las que las autoridades están facultadas para recurrir a tales medidas, en particular, precisando claramente la naturaleza de las infracciones que pueden dar lugar a una orden de interceptación y la definición de las categorías de personas susceptibles de ver intervenidos sus teléfonos" (párrafo 243).

"Respecto a la naturaleza de las infracciones, el Tribunal subraya que la condición de previsibilidad no obliga a los Estados a enunciar exhaustivamente, por su nombre, las infracciones específicas que pueden dar lugar a una interceptación. Sin embargo, deben proporcionarse detalles suficientes sobre la naturaleza de los delitos en cuestión (véase Kennedy). Tanto la OSAA como el CCrP establecen que las comunicaciones telefónicas y de otro tipo pueden ser interceptadas en relación con un delito de gravedad media, un delito grave o un delito especialmente grave —es decir, un delito para el que el Código Penal prescriba una pena máxima de más de tres años de

prisión— que ya se haya cometido, se esté cometiendo o se esté tramando. El Tribunal considera que la naturaleza de los delitos que pueden dar lugar a una orden de interceptación es suficientemente clara. Al mismo tiempo, observa con preocupación que la legislación rusa permite la interceptación secreta de comunicaciones en relación con una gama muy amplia de infracciones penales, incluido, por ejemplo, como señala el demandante, el hurto de carteras (véase para un razonamiento similar, *Iordachi y otros*)" (párrafo 244).

"El Tribunal también observa que, además de las interceptaciones con fines de prevención o detección de infracciones penales, la OSAA también establece que las comunicaciones telefónicas o de otro tipo pueden ser interceptadas tras la recepción de información sobre acontecimientos o actividades que pongan en peligro la seguridad nacional, militar, económica o ecológica de Rusia. La legislación rusa no define en ninguna parte qué acontecimientos o actividades pueden considerarse que ponen en peligro estos tipos de intereses de seguridad" (párrafo 246).

"[E]l Tribunal no pierde de vista que en Rusia es necesaria una autorización judicial previa para las interceptaciones. Dicha autorización judicial puede servir para limitar la discrecionalidad de las autoridades policiales a la hora de interpretar los amplios términos de ´una persona que pueda tener información sobre un delito´, ´una persona que pueda tener información relevante para la causa penal´ y ´acontecimientos o actividades que pongan en peligro la seguridad nacional, militar, económica o ecológica de Rusia´, siguiendo una interpretación judicial establecida de los términos o una práctica establecida para verificar si existen razones suficientes para interceptar las comunicaciones de un individuo concreto en cada caso. El Tribunal admite que la exigencia de autorización judicial previa constituye una importante salvaguardia contra la arbitrariedad. A continuación, se examinará la eficacia de dicha salvaguardia" (párrafo 249).

4. Vigilancia electrónica. Control judicial. Medidas de seguridad. Principio de proporcionalidad.

"Respecto a la primera salvaguardia, tanto el CCrP como la OSAA prevén que las interceptaciones puedan ser autorizadas por un juez por un período no superior a seis meses. Por lo tanto, existe una indicación clara en la legislación nacional del período tras el cual expirará una autorización de interceptación. En segundo lugar, las condiciones en las que puede renovarse una autorización también están claramente establecidas en la ley. En particular, tanto en virtud del CCrP como de la OSAA, un juez puede prorrogar la interceptación por un máximo de seis meses cada vez, tras un nuevo examen de todos los materiales pertinentes. Sin embargo, por lo que se refiere a la tercera salvaguardia relativa a las circunstancias en las que debe interrumpirse la intervención, el Tribunal observa que el requisito de interrumpir la intervención cuando ya no sea necesaria sólo se menciona en el CCrP. Lamentablemente, la OSAA no contiene tal requisito. En la práctica, esto significa que las interceptaciones en el marco de procedimientos penales cuentan con más salvaguardias que las interceptaciones realizadas fuera de dicho marco, en particular en relación con ´acontecimientos o actividades que pongan en peligro la seguridad nacional, militar, económica o ecológica´" (párrafo 251).

"El Tribunal concluye de lo anterior que, mientras que la legislación rusa contiene normas claras sobre la duración y la renovación de las interceptaciones que ofrecen garantías adecuadas contra los abusos, las disposiciones de la OSAA sobre la interrupción de las medidas de vigilancia no ofrecen garantías suficientes contra las injerencias arbitrarias" (párrafo 252).

5. Protección de datos personales. Prueba. Prueba digital. Derecho a la privacidad. Principio de reserva. Control judicial.

"La legislación rusa estipula que los datos recogidos como resultado de las medidas de vigilancia secreta constituyen un secreto de Estado y deben ser sellados y almacenados en condiciones que excluyan cualquier riesgo de acceso no autorizado. Pueden revelarse a aquellos funcionarios del

Estado que realmente necesiten los datos para el desempeño de sus funciones y tengan el nivel adecuado de habilitación de seguridad. Deberán tomarse medidas para garantizar que sólo se revele la cantidad de información que el destinatario necesite para desempeñar sus funciones, y no más. El funcionario responsable de garantizar que los datos se almacenan de forma segura y son inaccesibles para quienes no tienen la habilitación de seguridad necesaria está claramente definido. La legislación nacional también establece las condiciones y procedimientos para comunicar a las autoridades judiciales los datos interceptados que contengan información sobre un delito. Describe, en particular, los requisitos para su almacenamiento seguro y las condiciones para su utilización como prueba en procedimientos penales. El Tribunal está convencido de que la legislación rusa contiene normas claras que regulan el almacenamiento, la utilización y la comunicación de los datos interceptados, lo que permite reducir al mínimo el riesgo de acceso o divulgación no autorizados (véase, para un razonamiento similar, la sentencia *Kennedy*)" (párrafo 253).

"Respecto a los casos en los que la persona en cuestión no ha sido acusada de un delito penal, al Tribunal no le convence el argumento del demandante de que la legislación rusa permite el almacenamiento del material interceptado más allá del plazo legal. Parece que la disposición a la que se refiere el demandante no se aplica al caso concreto del almacenamiento de datos recogidos como resultado de la interceptación de comunicaciones. El Tribunal considera razonable el plazo de almacenamiento de seis meses establecido en la legislación rusa para dichos datos. Al mismo tiempo, lamenta que no se exija la destrucción inmediata de los datos que no sean pertinentes para el fin para el que se han obtenido (compárense las sentencias *Klass y otros* y *Kennedy*). El almacenamiento automático durante seis meses de datos claramente irrelevantes no puede considerarse justificado en virtud del artículo 8" (párrafo 255).

"Respecto a los casos en los que la persona ha sido acusada de un delito penal, el Tribunal observa con preocupación que la legislación rusa permite una discrecionalidad ilimitada al juez de primera instancia para almacenar o destruir los datos utilizados como prueba una vez finalizado el juicio. La legislación rusa no ofrece a los ciudadanos ninguna indicación sobre las circunstancias en las que el material interceptado puede almacenarse una vez finalizado el juicio. Por tanto, el Tribunal considera que la legislación interna no es suficientemente clara en este punto" (párrafo 256).

6. Control judicial. Vigilancia electrónica. Principio de legalidad. Principio de proporcionalidad. Derecho de defensa. Motivación.

"La legislación rusa contiene una importante salvaguardia contra la vigilancia secreta arbitraria o indiscriminada. Establece que toda interceptación de comunicaciones telefónicas o de otro tipo debe ser autorizada por un tribunal. El organismo encargado de hacer cumplir la ley que solicite autorización para la interceptación debe presentar una solicitud motivada a tal efecto a un juez, que puede exigir al organismo que presente material justificativo. El juez deberá motivar la decisión de autorizar las escuchas" (párrafo 259).

"El Tribunal señala que en Rusia el escrutinio judicial tiene un alcance limitado. Así, los materiales que contienen información sobre agentes encubiertos o informadores de la policía o sobre la organización y las tácticas de las medidas de búsqueda operativa no pueden presentarse al juez y, por lo tanto, están excluidos del ámbito de revisión del tribunal. El Tribunal considera que la no comunicación de la información pertinente a los órganos jurisdiccionales priva a éstos de la facultad de apreciar si existe una base fáctica suficiente para sospechar que la persona respecto de la cual se solicitan medidas de búsqueda operativa comete un delito o realiza actividades que ponen en peligro la seguridad nacional, militar, económica o ecológica (véase, *mutatis mutandis*, *Liu*). El Tribunal ha declarado anteriormente que existen técnicas que pueden emplearse para responder a preocupaciones legítimas de seguridad sobre la naturaleza y las fuentes de la información de los servicios de inteligencia y, al mismo tiempo, conceder a la persona un grado sustancial de justicia procesal (véase, *mutatis mutandis*, *Chahal v. el Reino Unido*)" (párrafo 261).

“[E]l Tribunal observa que la legislación interna no exige explícitamente a los tribunales de jurisdicción general a seguir la opinión de la Corte Constitucional sobre cómo debe interpretarse una disposición legislativa si dicha opinión se ha expresado en una decisión y no en una sentencia. De hecho, los materiales presentados por el demandante demuestran que los tribunales nacionales no siempre siguen las recomendaciones de la Corte Constitucional antes mencionadas, todas ellas contenidas en decisiones y no en sentencias. Así, de las notas analíticas emitidas por los Tribunales de Distrito se desprende que las solicitudes de interceptación no suelen ir acompañadas de ningún material justificativo, que los jueces de estos Tribunales de Distrito nunca solicitan a la agencia de interceptación que presente dicho material y que la mera referencia a la existencia de información sobre un delito penal o actividades que pongan en peligro la seguridad nacional, militar, económica o ecológica se considera suficiente para que se conceda la autorización. Una solicitud de interceptación sólo se rechaza si no está firmada por una persona competente, no contiene ninguna referencia al delito en relación con el cual se va a ordenar la interceptación, o se refiere a un delito penal respecto del cual la interceptación no está permitida por la legislación interna. Así, las notas analíticas emitidas por los Tribunales de Distrito, junto con la información estadística para el período comprendido entre 2009 y 2013 proporcionada por el solicitante, indican que en su práctica diaria los tribunales rusos no verifican si existe una ´sospecha razonable´ contra la persona en cuestión y no aplican la prueba de ´necesidad´ y ´proporcionalidad´” (párrafo 263).

“El Tribunal observa que el CCrP exige que una solicitud de autorización de interceptación mencione claramente a una persona concreta cuyas comunicaciones vayan a interceptarse, así como la duración de la medida de interceptación. En cambio, la OSAA no contiene ningún requisito en relación con el contenido de la solicitud de interceptación ni con el contenido de la autorización de interceptación. Como consecuencia de ello, los tribunales conceden a veces autorizaciones de interceptación que no mencionan a una persona o un número de teléfono concretos que deban intervenirse, sino que autorizan la interceptación de todas las comunicaciones telefónicas en la zona en la que se ha cometido un delito. Algunas autorizaciones no mencionan la duración de la interceptación autorizada. El Tribunal considera que tales autorizaciones, que no están claramente prohibidas por la OSAA, conceden un margen de apreciación muy amplio a las autoridades policiales en cuanto a qué comunicaciones interceptar y durante cuánto tiempo” (párrafo 265).

“El Tribunal señala además que, en casos urgentes, es posible interceptar comunicaciones sin autorización judicial previa durante un máximo de cuarenta y ocho horas. En tal caso, el juez debe ser informado en un plazo de veinticuatro horas a partir del inicio de la interceptación. Si no se ha emitido ninguna autorización judicial en el plazo de cuarenta y ocho horas, la interceptación debe detenerse inmediatamente). El Tribunal ya ha examinado el procedimiento de ´urgencia´ previsto en la legislación búlgara y ha considerado que era compatible con el Convenio (véase *Asociación para la Integración Europea y los Derechos Humanos* y *Ekimdzhiev*). Sin embargo, a diferencia de la disposición búlgara, el ´procedimiento de urgencia´ ruso no prevé suficientes salvaguardias para garantizar que se utilice con moderación y sólo en casos debidamente justificados. Así, aunque en el ámbito penal la OSAA limita el recurso al procedimiento de urgencia a los casos en los que existe un peligro inmediato de que se cometa un delito grave o especialmente grave, no contiene ninguna limitación de este tipo por lo que respecta a la vigilancia secreta en relación con acontecimientos o actividades que pongan en peligro la seguridad nacional, militar, económica o ecológica. La legislación nacional no limita el uso del procedimiento de urgencia a los casos que implican un peligro grave e inmediato para la seguridad nacional, militar, económica o ecológica. Deja a las autoridades un grado ilimitado de discrecionalidad para determinar en qué situaciones está justificado utilizar el procedimiento de urgencia no judicial, creando así posibilidades de recurrir a él de forma abusiva. Además, aunque la legislación rusa exige que se informe inmediatamente a un juez de cada caso de interceptación urgente, su poder se limita a autorizar

la prórroga de la medida de interceptación más allá de cuarenta y ocho horas. No tiene poder para evaluar si el uso del procedimiento urgente estaba justificado o para decidir si el material obtenido durante las cuarenta y ocho horas anteriores debe conservarse o destruirse (véase, por el contrario, *Asociación para la Integración Europea y los Derechos Humanos* y *Ekimdzhiev*). Por lo tanto, la legislación rusa no prevé un control judicial efectivo del procedimiento de urgencia" (párrafo 266).

"Por tanto, el Tribunal estima que los procedimientos de autorización previstos por la legislación rusa no son capaces de garantizar que las medidas de vigilancia secreta no se ordenen de forma fortuita, irregular o sin la debida y adecuada consideración" (párrafo 267).

7. Vigilancia electrónica. Control judicial. Derecho la privacidad. Principio de proporcionalidad.

"El Tribunal considera que el requisito de mostrar una autorización de interceptación al proveedor de servicios de comunicaciones antes de obtener acceso a las comunicaciones de una persona es una de las salvaguardias importantes contra el abuso por parte de las autoridades encargadas de hacer cumplir la ley, garantizando que se obtenga la autorización adecuada en todos los casos de interceptación. La legislación rusa no exige a las autoridades policiales que muestren la autorización judicial al proveedor de servicios de comunicaciones antes de obtener acceso a las comunicaciones de una persona (véase, por el contrario, *la Resolución del Consejo de la UE*), excepto en relación con el control de los datos relacionados con las comunicaciones en virtud de la CCrP. De hecho, de conformidad con las Órdenes emitidas por el Ministerio de Comunicaciones, en particular las adiciones a la Orden núm. 70, los proveedores de servicios de comunicaciones deben instalar equipos que den a las autoridades encargadas de hacer cumplir la ley acceso directo a todas las comunicaciones de telefonía móvil de todos los usuarios. Los proveedores de servicios de comunicaciones también tienen la obligación, en virtud de la Orden núm. 538 de crear bases de datos que almacenen información sobre todos los abonados, y los servicios que se les prestan, durante tres años; los servicios secretos tienen acceso directo a distancia a esas bases de datos. De este modo, las fuerzas del orden tienen acceso directo a todas las comunicaciones de telefonía móvil y a los datos de las comunicaciones correspondientes" (párrafo 269).

"El Tribunal considera que el funcionamiento del sistema de vigilancia secreta en Rusia proporciona a los servicios de seguridad y a la policía los medios técnicos para eludir el procedimiento de autorización e interceptar cualquier comunicación sin obtener autorización judicial previa. Aunque nunca puede excluirse por completo la posibilidad de una actuación indebida por parte de un funcionario deshonesto, negligente o excesivamente celoso, cualquiera que sea el sistema (véase *Klass y otros*), el Tribunal considera que un sistema, como el ruso, que permite a los servicios secretos y a la policía interceptar directamente las comunicaciones de todos y cada uno de los ciudadanos sin exigirles que muestren una autorización de interceptación al proveedor de servicios de comunicaciones, o a cualquier otra persona, es especialmente propenso a los abusos. La necesidad de salvaguardias contra la arbitrariedad y el abuso parece, por tanto, especialmente grande" (párrafo 270).

"Por consiguiente, el Tribunal examinará con especial atención si el dispositivo de control previsto por la legislación rusa es capaz de garantizar que todas las interceptaciones se realicen legalmente sobre la base de una autorización judicial adecuada" (párrafo 271).

8. Control judicial. Vigilancia electrónica. Derecho a la información. Principio de legalidad.

"El Tribunal señala en primer lugar que la Orden nº. 70 exige que los equipos instalados por los proveedores de servicios de comunicaciones no graben ni registren información sobre las interceptaciones. El Tribunal ha considerado que la obligación de los organismos de interceptación de mantener registros de las interceptaciones es especialmente importante para garantizar que el organismo de supervisión tenga acceso efectivo a los detalles de las actividades de vigilancia

realizadas (véase la sentencia *Kennedy*). La prohibición de registrar o grabar interceptaciones establecida en la legislación rusa imposibilita que la autoridad supervisora descubra las escuchas realizadas sin la debida autorización judicial. En combinación con la capacidad técnica de las autoridades encargadas de hacer cumplir la ley de interceptar directamente todas las comunicaciones, esta disposición hace que cualquier mecanismo de supervisión sea incapaz de detectar las interceptaciones ilegales y, por lo tanto, ineficaz" (párrafo 272).

"El tribunal que ha concedido la autorización de interceptación no tiene competencia para supervisar su aplicación. No se le informa de los resultados de las interceptaciones y no tiene competencia para revisar si se cumplieron los requisitos de la decisión por la que se concedió la autorización. Los tribunales rusos en general tampoco tienen competencia para llevar a cabo la supervisión general de las interceptaciones. La supervisión judicial se limita a la fase inicial de autorización. La supervisión posterior se confía al presidente, al Parlamento, al Gobierno, el fiscal general y los fiscales competentes de rango inferior" (párrafo 274).

"En cuanto a la supervisión de las interceptaciones por parte de los fiscales, el Tribunal observa que la legislación rusa establece el ámbito de aplicación y los procedimientos de supervisión por parte de los fiscales de las actividades operativas de búsqueda. Establece que los fiscales pueden llevar a cabo inspecciones rutinarias y *ad hoc* de los organismos que realizan actividades de búsqueda operativa y tienen derecho a estudiar los documentos pertinentes, incluidos los confidenciales. Pueden tomar medidas para poner fin o remediar las infracciones de la ley detectadas y hacer que los responsables rindan cuentas. Deben presentar informes semestrales con los resultados de las inspecciones a la fiscalía general. El Tribunal acepta que existe un marco jurídico que prevé, al menos en teoría, una cierta supervisión de las medidas de vigilancia secreta por parte de los fiscales. A continuación, debe examinarse si los fiscales son independientes de las autoridades que llevan a cabo la vigilancia, y están investidos con poderes y competencias suficientes para ejercer un control efectivo y continuo" (párrafo 277).

"[E]l Tribunal señala que es esencial que el órgano de control tenga acceso a todos los documentos pertinentes, incluidos los materiales cerrados, y que todos los implicados en las actividades de interceptación tengan el deber de revelarle cualquier material que requiera (véase *Kennedy*). La legislación rusa estipula que los fiscales tienen derecho a estudiar los documentos pertinentes, incluidos los confidenciales. Sin embargo, es importante señalar que la información sobre los agentes encubiertos de los servicios de seguridad, y sobre las tácticas, métodos y medios utilizados por ellos, queda fuera del ámbito de supervisión de los fiscales. Por lo tanto, el alcance de su supervisión es limitado. Además, las interceptaciones realizadas por el FSB [*Federal Security Service*] en el ámbito del contraespionaje sólo pueden inspeccionarse previa denuncia individual. Dado que las interceptaciones no se notifican a los particulares, es poco probable que se presente nunca una denuncia de este tipo. En consecuencia, las medidas de vigilancia relacionadas con la contrainteligencia escapan de facto a la supervisión de los fiscales" (párrafo 281).

"El Tribunal también debe examinar si las actividades del órgano de control de supervisión están abiertas al escrutinio público (véase, por ejemplo, *L. v. Norway*, donde la supervisión fue realizada por el Comité de Control que informaba anualmente al Gobierno y cuyos informes eran publicados y debatidos por el Parlamento; *Kennedy*, antes citada, apartado 166, donde la supervisión de las interceptaciones corría a cargo del Comisario de Comunicaciones, que informaba anualmente al Primer Ministro, siendo su informe un documento público presentado ante el Parlamento; y, por el contrario, *Association for European Integration and Human Rights* y *Ekimdzhiev,* en la que el Tribunal encontró fallos en el sistema en el que ni el Ministro del Interior ni ningún otro funcionario estaba de informar regularmente a un órgano independiente o al público en general sobre el funcionamiento general del sistema o sobre las medidas aplicadas en casos individuales). En Rusia, los fiscales deben presentar informes semestrales detallando los resultados de las inspecciones a la fiscalía general. Sin embargo, estos informes se refieren a todos

los tipos de medidas de búsqueda operativa, amalgamadas, sin que las interceptaciones se traten por separado de otras medidas. Además, los informes sólo contienen información estadística sobre el número de inspecciones de medidas de búsqueda operativa realizadas y el número de infracciones detectadas, sin especificar la naturaleza de las infracciones ni las medidas adoptadas para subsanarlas. También es significativo que los informes sean documentos confidenciales. No se publican ni son accesibles al público. De ello se deduce que en Rusia la supervisión por parte de los fiscales se lleva a cabo de una manera que no está abierta al escrutinio y conocimiento públicos" (párrafo 283).

"En vista de los defectos identificados [...], y teniendo en cuenta la especial importancia de la supervisión en un sistema en el que las fuerzas de seguridad las autoridades policiales tienen acceso directo a todas las comunicaciones, el Tribunal considera que la supervisión de las interceptaciones por parte de los fiscales, tal como está organizada actualmente no puede ofrecer garantías adecuadas y eficaces contra los abusos" (párrafo 285).

9. Derecho a la información. Acceso a la justicia. Derecho de defensa. Prueba digital. Carga de la prueba. Recursos judiciales.

"[E]l Tribunal observa que en Rusia las personas cuyas comunicaciones han sido interceptadas no son notificadas de este hecho en ningún momento ni en ninguna circunstancia. De ello se deduce que, a menos que se haya incoado un procedimiento penal contra el sujeto interceptado y que los datos interceptados se hayan utilizado como prueba, o a menos que se haya producido una filtración, es improbable que el interesado llegue a enterarse de que sus comunicaciones han sido interceptadas" (párrafo 289).

"El Tribunal toma nota del hecho de que una persona que de algún modo ha tenido conocimiento de que sus comunicaciones han sido interceptadas puede solicitar información sobre los datos correspondientes. Cabe señalar a este respecto que, para tener derecho a presentar dicha solicitud, la persona debe estar en posesión de los hechos de las medidas de búsqueda operativa a las que fue sometida. De ello se deduce que el acceso a la información está condicionado a que la persona pueda probar que sus comunicaciones fueron interceptadas. Además, el sujeto interceptado no tiene derecho a obtener acceso a los documentos relativos a la interceptación de sus comunicaciones; en el mejor de los casos, tiene derecho a recibir ´información´ sobre los datos recogidos. Dicha información sólo se proporciona en circunstancias muy limitadas, a saber, si no se ha demostrado la culpabilidad de la persona de conformidad con el procedimiento prescrito por la ley, es decir, si no ha sido acusada o se han retirado los cargos por no haberse cometido el presunto delito o por faltar uno o más elementos de un delito penal. También es significativo que sólo la información que no contenga secretos de Estado puede ser revelada al sujeto interceptado y que, según la legislación rusa, la información sobre las instalaciones utilizadas en las actividades de búsqueda operativa, los métodos empleados, los funcionarios implicados y los datos recogidos constituye un secreto de Estado. A la vista de las anteriores características de la legislación rusa, la posibilidad de obtener información sobre las interceptaciones parece ser ineficaz" (párrafo 290).

"El primero de los procedimientos invocados por el Gobierno es un recurso de apelación, de casación o de revisión contra la resolución judicial que autoriza la intervención de las comunicaciones. Sin embargo, la Corte Constitucional declaró claramente que el sujeto interceptado no tiene derecho a recurrir la decisión judicial que autoriza la interceptación de sus comunicaciones. La legislación interna no se pronuncia sobre la posibilidad de interponer un recurso de casación. Dado que el Gobierno no presentó ningún ejemplo de práctica interna sobre el examen de los recursos de casación, el Tribunal tiene serias dudas sobre la existencia de un derecho a interponer un recurso de casación contra una resolución judicial que autorice la interceptación de las comunicaciones. Al mismo tiempo, es evidente que la persona interceptada tiene derecho a interponer un recurso de revisión. Sin embargo, para interponer un recurso de

control contra la resolución judicial que autoriza la intervención de las comunicaciones, el interesado debe tener conocimiento de la existencia de dicha resolución. Aunque la Corte Constitucional ha declarado que no es necesario adjuntar una copia de la resolución judicial impugnada a la reclamación de control, es difícil imaginar cómo una persona puede presentar dicha reclamación sin tener al menos la información mínima sobre la resolución que impugna, como su fecha y el órgano jurisdiccional que la ha dictado. A falta de notificación de las medidas de vigilancia con arreglo a la legislación rusa, un particular difícilmente podría obtener esa información, a menos que fuera revelada en el contexto de un proceso penal contra él o que hubiera habido alguna indiscreción que haya dado lugar a su divulgación" (párrafo 294).

"Respecto a la reclamación de revisión judicial en virtud de la Ley de revisión judicial, el capítulo 25 del Código de Procedimiento Penal y el nuevo Código de Procedimiento Administrativo, y a la reclamación de responsabilidad civil extracontractual en virtud del artículo 1069 del Código Civil, la carga de la prueba recae en el demandante, que debe demostrar que se ha producido la interceptación y que con ello se han vulnerado sus derechos. En ausencia de notificación o de alguna forma de acceso a los documentos oficiales relativos a las interceptaciones, dicha carga de la prueba es prácticamente imposible de satisfacer. De hecho, la reclamación judicial del demandante fue desestimada por los tribunales nacionales por no haber probado que sus comunicaciones telefónicas habían sido interceptadas. El Tribunal observa que el Gobierno presentó varias decisiones judiciales adoptadas en virtud del capítulo 25 del CPC o del artículo 1069 del Código Civil. Sin embargo, todas esas decisiones, con una excepción, se refieren a registros o incautaciones de documentos u objetos, es decir, a medidas de búsqueda operativa llevadas a cabo con el conocimiento de la persona afectada. Sólo una decisión judicial se refiere a la interceptación de comunicaciones. En ese caso, la persona interceptada pudo liberarse de la carga de la prueba porque había tenido conocimiento de la interceptación de sus comunicaciones en el curso de un procedimiento penal contra ella" (párrafo 296).

"El Tribunal concluye [...] que los recursos mencionados por el Gobierno sólo están disponibles para las personas que están en posesión de información sobre la interceptación de sus comunicaciones. Por lo tanto, su eficacia se ve socavada por la ausencia de la obligación de notificar al sujeto de la interceptación en cualquier momento, o de una posibilidad adecuada de solicitar y obtener información sobre las interceptaciones de las autoridades. En consecuencia, el Tribunal declara que la legislación rusa no prevé un recurso judicial efectivo contra las medidas de vigilancia secreta en los casos en que no se haya incoado un procedimiento penal contra el sujeto interceptado. No es tarea del Tribunal en el presente caso decidir si estos recursos serán efectivos en los casos en que un individuo se entere de la interceptación de sus comunicaciones en el curso de un proceso penal contra él (véase *Avanesyan*, donde se consideró que algunos de estos recursos no eran efectivos para denunciar una "inspección" del piso del demandante)" (párrafo 298).

"[E]l Tribunal constata que la legislación rusa no prevé recursos efectivos para una persona que sospeche que ha sido objeto de una vigilancia secreta. Al privar al sujeto de la interceptación de la posibilidad efectiva de impugnar retrospectivamente las interceptaciones, la legislación interna prescinde así de una importante salvaguardia contra el uso indebido de las medidas de vigilancia secreta" (párrafo 300).

"Por las razones anteriores, el Tribunal también rechaza la objeción del Gobierno en cuanto a la falta de agotamiento de los recursos internos" (párrafo 301).

2.4. TRIBUNAL EUROPEO DE DERECHOS HUMANOS (TEDH), "BEN FAIZA V. FRANCIA". CASO N° 31446/12. 8/5/2018.

HECHOS

Un hombre estaba siendo investigado por presuntos delitos de tráfico de estupefacientes y narcotráfico después de una denuncia anónima. La policía francesa solicitó a la fiscalía obtener información de una empresa de telefonía móvil para identificar llamadas y rastrear la ubicación de cuatro números. Posteriormente, la fiscalía hizo la presentación ante un juzgado de instrucción. El tribunal de grado autorizó la interceptación de datos telefónicos y la colocación de un dispositivo de seguimiento en un auto utilizado por el sospechoso y sus hermanos. Los resultados mostraron que dirigían operaciones relacionadas con los delitos investigados, incluida la importación de drogas de los Países Bajos. Tras confirmarse la importación de estupefacientes a gran escala, se solicitó autorización para instalar un dispositivo de geolocalización (GPS) en el vehículo de los sospechosos, lo que llevó a su detención. Contra esa medida, la defensa presentó un recurso ante la Corte de Casación. Para ello, la defensa argumentó que las medidas eran ilegales según el Convenio Europeo de Derechos Humanos. En tal sentido, sostuvo que el uso de un dispositivo GPS junto con las escuchas telefónicas y la captura de imágenes constituía una intromisión en la vida de su asistido, toda vez que no existía una norma en el ámbito interno que permitiera la vigilancia mediante un GPS en particular. Sin embargo, la Corte de Casación, desestimó el recurso, y convalidó la requisa judicial.

DECISIÓN

El Tribunal Europeo de Derechos Humanos consideró que Francia era responsable por la violación del artículo 8 del Convenio Europeo de Derechos Humanos con respecto a la medida de geolocalización al colocar un dispositivo GPS en el vehículo.

ARGUMENTOS

1. Derecho a la privacidad. Principio de legalidad. Razonabilidad. Principio de proporcionalidad. Protección de datos personales. Espacio público. Vigilancia electrónica. Control judicial. Control de constitucionalidad. Democracia.

"El Gobierno no niega que la implementación de un dispositivo de geolocalización en el vehículo, combinado con escuchas telefónicas, constituye una intromisión en la vida privada del solicitante. Sin embargo, considera que esta intromisión estaba prevista por la ley, perseguía un fin legítimo y era necesaria en una sociedad democrática" (párrafo 50).

"[A]unque en la fecha de la sentencia de la Corte de Casación no se preveía expresamente en el CPP [Código de Procedimiento Penal] la posibilidad de recurrir a la geolocalización mediante un dispositivo GPS, esta técnica de investigación era posible en virtud del artículo 81 del CPP. Además, destaca que la colocación del GPS fue autorizada por el juez de instrucción, un magistrado independiente, por un período de un mes. Subraya también que esta vigilancia se ordenó después de que se implementaran otras medidas de observación (vigilancia visual por parte de agentes de policía, instalación de dispositivos de captación de imágenes, intercepciones telefónicas). Argumenta que la orden estaba debidamente fundamentada, con el aval de la fiscalía, y que todas las operaciones se registraron en un acta y se llevaron a cabo bajo el control continuo y regular del juez. Destaca que los tribunales penales pudieron controlar la legalidad de dicha medida de vigilancia en el marco del procedimiento contra el solicitante, así como su proporcionalidad" (párrafo 51).

“[El Tribunal], recuerda que el dispositivo GPS tenía como objetivos la prevención de delitos penales, la seguridad nacional y la seguridad pública, objetivos contemplados en el artículo 8, párrafo 2, de la Convención” (párrafo 52).

"El Tribunal observa que la geolocalización en tiempo real es una técnica especial de investigación que permite rastrear en directo los movimientos de una persona o un objeto. Hay dos formas de llevarlo a cabo: por un lado, el seguimiento dinámico de un terminal de telecomunicaciones, utilizando la tecnología propia de un teléfono, una tableta o un vehículo equipado con un sistema GPS; por otro lado, un dispositivo físico instalado directamente en un medio de transporte u otro objeto, como una baliza. El Tribunal recuerda que es importante distinguir, por su naturaleza, la vigilancia mediante geolocalización de otros métodos de vigilancia a través de medios visuales o acústicos que, por lo general, son más propensos a violar el derecho de una persona al respeto de su vida privada, ya que revelan más información sobre la conducta, opiniones o sentimientos de la persona en cuestión (*Uzun v. Alemania*). No obstante, el Tribunal ya ha dictaminado que la vigilancia de una persona a través de GPS, así como el tratamiento y uso de los datos obtenidos de esta manera, constituyen una interferencia en la vida privada de esa persona, protegida por el artículo 8, párrafo 1 (*Uzun*, citado)” (párrafo 53).

“[E]l Tribunal observa que la implementación de un sistema de geolocalización en el vehículo utilizado por el solicitante y el uso de los datos obtenidos de esta medida permitieron a los investigadores conocer, en tiempo real, los movimientos del solicitante y saber que había viajado a los Países Bajos, lo que llevó a su arresto. Además, señala que esta medida de geolocalización estaba vinculada a la implementación de un dispositivo técnico que permitía capturar, fijar, transmitir y grabar las conversaciones de las personas dentro de ese vehículo, sometiendo así al solicitante a una vigilancia particularmente estrecha” (párrafo 54).

“[E]l Tribunal considera que la geolocalización mediante la colocación de un receptor GPS en el vehículo del solicitante, así como el tratamiento y uso de los datos obtenidos constituyen una interferencia en la vida privada del interesado, tal como lo protege el artículo 8, párrafo 1 del Convenio” (párrafo 55).

“El Tribunal considera que las palabras ´previstas por ley´, en el sentido del artículo 8, párrafo 2, implican en primer lugar que la medida incriminada tenga una base legal en el derecho interno. Para determinar si existe tal ´base legal´, se debe tener en cuenta no solo los textos legislativos pertinentes, sino también la jurisprudencia (ver, en particular, *Kruslin v. Francia*, *Huvig v. Francia*, y *Wisse v. Francia*)” (párrafo 56).

“[El Tribunal] recuerda que en la sentencia *Uzun*, se consideró que la intromisión en el derecho al respeto de la vida privada del solicitante, resultante de su vigilancia por GPS, tenía una base en la legislación alemana, a saber, el artículo 100 c 1.1 b) del CPP que establecía lo siguiente: ´Es posible, sin el conocimiento del interesado, (...) recurrir a otros medios técnicos especiales destinados a la vigilancia con el fin de investigar los hechos del caso o localizar al autor de un delito cuando la investigación involucra un delito extremadamente grave, y cuando otros medios de investigación de los hechos del caso o de localización del autor del delito tienen menos posibilidades de tener éxito o son más difíciles de implementar (...)´ (párrafo 57).

“A diferencia de la disposición del derecho alemán, el artículo 81 del CPP, aplicado en este caso, hace referencia simplemente a una noción muy general, es decir, ´actos de información que considere útiles para la manifestación de la verdad´. Además, el Tribunal recuerda que ya ha dictaminado, en casos relacionados con escuchas telefónicas, que el artículo 81 del CPP, incluso leído en combinación con otras disposiciones del CPP, no ofrecía la ´previsibilidad´ exigida por el artículo 8 del Convenio (ver casos *Kruslin y Huvig*, citados anteriormente). El hecho de que la

vigilancia de los desplazamientos por GPS constituya una interferencia menos intrusiva en la vida privada que la interceptación de conversaciones telefónicas (ver caso *Uzun*), no es, en sí mismo, motivo para cuestionar esta constatación, especialmente porque se sumó a otras medidas de observación (ver caso *Uzun*). Además, el Tribunal observa que la imprecisión de la ley francesa en el momento de los hechos no puede ser compensada por la jurisprudencia de los tribunales nacionales, siendo la sentencia de la Corte de Casación, dictada en este caso el 22 de noviembre de 2011, la primera en pronunciarse sobre la legalidad de la geolocalización durante una investigación judicial" (párrafo 58).

"[E]l Tribunal considera que, aunque el artículo 81 del CPP pudiera haber sido en sí mismo una base legal para la geolocalización, está también debería haber cumplido con los criterios de previsibilidad y la existencia de garantías adecuadas y suficientes contra el riesgo de abuso inherente a todo sistema de vigilancia secreta. Sin embargo, en este punto, el Tribunal observa que tales garantías no se desprenden ni de los términos del artículo 81 del CPP ni de la jurisprudencia interna" (párrafo 59).

"Estos elementos son suficientes para que el Tribunal considere que, en el ámbito de las medidas de geolocalización, el derecho francés, tanto escrito como no escrito, no indicaba con suficiente claridad, en el momento de los hechos en cuestión, la extensión y las modalidades de ejercicio del poder de apreciación de las autoridades en el ámbito considerado. Concluye que el demandante no ha disfrutado del grado mínimo de protección deseado por la primacía del derecho en una sociedad democrática y, por lo tanto, ha habido una violación del artículo 8 de la Convención, sin necesidad de abordar las otras condiciones establecidas por el artículo 8, a saber, que la interferencia debe tener un fin legítimo y ser necesaria en una sociedad democrática" (párrafo 60).

2.5. TRIBUNAL EUROPEO DE DERECHOS HUMANOS, GRAN SALA, "BIG BROTHER WATCH Y OTROS V. EL REINO UNIDO". CASOS N° 58170/13, 62322/14 Y 24960/15. 25 /6/2021.

HECHOS

En junio de 2013, un ex consultor nacional de inteligencia informático de los Estados Unidos reveló la existencia de programas de vigilancia electrónica operados por los servicios de inteligencia de Estados Unidos y el Reino Unido. Como consecuencia, entre junio y diciembre de 2013, varios grupos de demandantes, incluyendo organizaciones no gubernamentales y periodistas, presentaron quejas ante el Tribunal de Poderes de Investigación (IPT) del Reino Unido. Los demandantes alegaron que el régimen de interceptación masiva del Reino Unido, conocido como el régimen de la sección 8(4) (TEMPORA), el intercambio de inteligencia con servicios extranjeros (*PRISM* y *Upstream*) y la adquisición de datos de comunicaciones de proveedores de servicios (CSPs) afectaban el derecho al respeto a la vida privada y familiar y la libertad de expresión, respectivamente. Posteriormente, en diciembre de 2014, el IPT resolvió que el régimen de interceptación masiva era en general compatible con el Convención Europea de Derechos Humanos. Sin embargo, en febrero de 2015, el IPT declaró que el régimen de interceptación masiva había sido ilegal antes de las revelaciones hechas durante el proceso judicial.

Frente a estas decisiones y luego de agotar los recursos internos, los demandantes hicieron las presentaciones ante el Tribunal Europeo de Derechos Humanos (TEDH) entre septiembre de 2013 y mayo de 2015. En sus peticiones, argumentaron que el régimen de la sección 8(4) carecía de una base legal adecuada y no proporcionaba salvaguardias suficientes contra el abuso. Asimismo, sostuvieron que la interceptación masiva constituía una interferencia desproporcionada con su derecho al respeto de su vida privada y familiar. Además, que la falta de supervisión independiente en la selección de los "selectores fuertes" y la ausencia de salvaguardias adecuadas para los datos de comunicaciones relacionados violaban sus derechos. Finalmente, cuestionaron el régimen de intercambio de inteligencia con servicios extranjeros, argumentando que carecía de salvaguardias suficientes y podría utilizarse para eludir las protecciones domésticas. Por su parte, el Gobierno del Reino Unido defendió la legalidad y proporcionalidad del régimen de interceptación masiva. Argumentó que la interceptación masiva era una capacidad vital para identificar nuevas amenazas y que el régimen contenía salvaguardias adecuadas. Finalmente, el Gobierno sostuvo que los Estados deberían tener un amplio margen de apreciación en asuntos de seguridad nacional y que el régimen cumplía con los requisitos del Convenio. En septiembre de 2018, la Sala del TEDH resolvió que el Gobierno del Reino Unido era responsable por la violación de los artículos 8 y 10 en relación con el régimen de interceptación masiva y el régimen de adquisición de datos de comunicaciones. Sin embargo, no encontró violación respecto al régimen de intercambio de inteligencia. Posteriormente, en febrero de 2019, el caso fue remitido a la Gran Sala del TEDH a petición de los demandantes. La Gran Sala celebró una audiencia pública el 10 de julio de 2019, en la que se presentaron argumentos adicionales.

DECISIÓN

La Gran Sala del Tribunal Europeo de Derechos Humanos consideró que Reino Unido era responsable por la violación del derecho al respeto de la vida privada y la correspondencia y la libertad de expresión, toda vez que el régimen de interceptación masiva no contenía salvaguardias suficientes, no contaba con una supervisión de la selección de selectores y por la falta de protección de los datos personales involucrados (artículos 8 y 10 del Convenio Europeo de Derechos Humanos).

ARGUMENTOS

1. Derecho a la privacidad. Vigilancia electrónica. Democracia. Principio de proporcionalidad. Sistema informático. Protección de datos personales.

“En el curso de los procedimientos se ha hecho evidente que la evaluación de cualquier régimen de este tipo enfrenta dificultades específicas. En la actual era cada vez más digital, la gran mayoría de las comunicaciones toman forma digital y son transportadas a través de redes globales de telecomunicaciones utilizando una combinación de las rutas más rápidas y baratas sin ninguna referencia significativa a las fronteras nacionales. Por lo tanto, la vigilancia que no está dirigida directamente a individuos tiene la capacidad de tener un alcance muy amplio, tanto dentro como fuera del territorio del Estado que realiza la vigilancia. Las salvaguardias son, por lo tanto, fundamentales y, sin embargo, difíciles de alcanzar. A diferencia de la interceptación dirigida, que ha sido objeto de gran parte de la jurisprudencia del Tribunal, y que se utiliza principalmente para la investigación de delitos, la interceptación masiva también se utiliza —quizás incluso predominantemente— para la recopilación de inteligencia extranjera y la identificación de nuevas amenazas tanto de actores conocidos como desconocidos. Cuando operan en este ámbito, los Estados Contratantes tienen una necesidad legítima de secreto que significa que poca, si es que alguna, información sobre el funcionamiento del esquema estará en el dominio público, y tal información como está disponible puede estar expresada en una terminología que es oscura y que puede variar significativamente de un Estado a otro” (párrafo 322).

“Mientras que las capacidades tecnológicas han aumentado enormemente el volumen de comunicaciones que atraviesan el Internet global, las amenazas que enfrentan los Estados contratantes y sus ciudadanos también han proliferado. Estas incluyen, pero no se limitan a, el terrorismo global, el tráfico de drogas, la trata de personas y la explotación sexual de niños. Muchas de estas amenazas provienen de redes internacionales de actores hostiles con acceso a tecnología cada vez más sofisticada que les permite comunicarse sin ser detectados. El acceso a dicha tecnología también permite a actores estatales y no estatales hostiles perturbar la infraestructura digital e incluso el propio funcionamiento de los procesos democráticos a través de ataques cibernéticos, una seria amenaza a la seguridad nacional que por definición existe solo en el dominio digital y como tal solo puede ser detectada e investigada allí. En consecuencia, se requiere que el Tribunal lleve a cabo su evaluación de los regímenes de interceptación masiva de los Estados contratantes, una valiosa capacidad tecnológica para identificar nuevas amenazas en el dominio digital, para el cumplimiento del Convenio por referencia a la existencia de salvaguardias contra la arbitrariedad y el abuso, sobre la base de información limitada sobre la manera en que operan esos regímenes" (párrafo 323).

“El Gobierno no disputa que ha habido una interferencia con los derechos de los demandantes en virtud del artículo 8 del Convenio, aunque alegaron que para los propósitos del artículo 8 del Convenio la única interferencia significativa podía haber ocurrido cuando las comunicaciones fueron seleccionadas para su examen” (párrafo 324).

“El Tribunal ve la interceptación masiva como un proceso gradual en el que el grado de interferencia con los derechos de los individuos bajo el artículo 8 aumenta a medida que el proceso avanza. Los regímenes de interceptación masiva pueden no seguir exactamente el mismo modelo, y las diferentes etapas del proceso no serán necesariamente discretas o seguidas en estricto orden cronológico. Sin embargo, sujeto a las advertencias mencionadas, el Tribunal considera que las etapas del proceso de interceptación masiva que deben considerarse pueden describirse de la siguiente manera: (a) la interceptación y retención inicial de comunicaciones y datos de comunicaciones relacionados (es decir, los datos de tráfico pertenecientes a las comunicaciones interceptadas); (b) la aplicación de selectores específicos a las comunicaciones/datos de comunicaciones relacionados retenidos; (c) el examen de las comunicaciones seleccionadas/datos de comunicaciones relacionados por analistas; y (d) la

posterior retención de datos y uso del ´producto final´, incluido el intercambio de datos con terceros" (párrafo 325).

"[E]l Tribunal ha tomado como la primera etapa, las comunicaciones electrónicas (o ´paquetes´ de comunicaciones electrónicas) que serán interceptadas en masa por los servicios de inteligencia. Estas comunicaciones pertenecerán a un gran número de individuos, muchos de los cuales no serán de interés alguno para los servicios de inteligencia. Algunas comunicaciones de un tipo que probablemente no sea de interés de inteligencia pueden filtrarse en esta etapa" (párrafo 326).

"La búsqueda inicial, que es principalmente automatizada, tiene lugar en lo que el Tribunal ha tomado como la segunda etapa, cuando se aplican diferentes tipos de selectores, incluidos ´selectores fuertes´ (como una dirección de correo electrónico) y/o consultas complejas a los paquetes retenidos de comunicaciones y datos de comunicaciones relacionados. Esta puede ser la etapa donde el proceso comienza a dirigirse a individuos a través del uso de selectores fuertes" (párrafo 327).

"En lo que el Tribunal ha tomado como la tercera etapa, el material interceptado es examinado por primera vez por un analista" (párrafo 328).

"Lo que el Tribunal ha tomado como la etapa final es cuando el material interceptado es realmente utilizado por los servicios de inteligencia. Esto puede implicar la creación de un informe de inteligencia, la difusión del material a otros servicios de inteligencia dentro del Estado interceptor, o incluso la transmisión de material a servicios de inteligencia extranjeros" (párrafo 329).

"El Tribunal considera que el artículo 8 se aplica en cada una de las etapas anteriores. Mientras que la interceptación inicial seguida del descarte inmediato de partes de las comunicaciones no constituye una interferencia particularmente significativa, el grado de interferencia con los derechos de privacidad de los individuos aumentará a medida que el proceso de interceptación masiva avanza. A este respecto, el Tribunal ha declarado claramente que incluso el mero almacenamiento de datos relativos a la vida privada de un individuo constituye una interferencia en el sentido del artículo 8 (ver *Leander v. Suecia*), y que la necesidad de salvaguardias será tanto mayor donde la protección de datos personales sometidos a procesamiento automático está en juego (ver *S. y Marper v. el Reino Unido* [GC]). El hecho de que el material almacenado esté en forma codificada, inteligible solo con el uso de tecnología informática y capaz de ser interpretado solo por un número limitado de personas, no puede tener incidencia en esa conclusión (ver *Amann v. Suiza* y *S. y Marper*). Finalmente, al final del proceso, donde la información sobre una persona en particular será analizada o el contenido de las comunicaciones está siendo examinado por un analista, la necesidad de salvaguardias estará en su punto más alto. Este enfoque del Tribunal está en línea con el hallazgo de la Comisión de Venecia, que en su informe sobre la Supervisión Democrática de las Agencias de Inteligencia de Señales consideró que en la interceptación masiva la principal interferencia con la privacidad ocurría cuando los datos personales almacenados eran procesados y/o accedidos por las agencias" (párrafo 330).

"[E]l grado de interferencia con los derechos de privacidad aumentará a medida que el proceso avanza a través de las diferentes etapas. Al examinar si esta creciente interferencia estaba justificada, el Tribunal llevará a cabo su evaluación del régimen de la sección 8(4) sobre la base de este entendimiento de la naturaleza de la interferencia" (párrafo 331).

"En *Weber y Saravia y Liberty y Otros*, el Tribunal aceptó que los regímenes de interceptación masiva no caían *per se* fuera del margen de apreciación de los Estados. En vista de la proliferación de amenazas que los Estados enfrentan actualmente de redes de actores internacionales, que utilizan Internet tanto para la comunicación como como herramienta, y la existencia de tecnología sofisticada que permitiría a estos actores evitar la detección, el Tribunal considera que la decisión

de operar un régimen de interceptación masiva para identificar amenazas a la seguridad nacional o contra intereses nacionales esenciales es una que continúa cayendo dentro de este margen" (párrafo 340).

“[M]ientras que la interceptación masiva en los casos de *Weber y Saravia y Liberty y Otros* era a simple vista similar a la del caso en cuestión, ambos casos tienen ahora más de diez años, y en los años intermedios los desarrollos tecnológicos han cambiado significativamente la forma en que las personas se comunican. Las vidas se viven cada vez más en línea, generando tanto un volumen significativamente mayor de comunicaciones electrónicas, como comunicaciones de una naturaleza y calidad significativamente diferentes a las que probablemente se generaban hace una década. El alcance de la actividad de vigilancia considerada en esos casos habría sido, por lo tanto, mucho más estrecho” (párrafo 341).

“Esto es igualmente cierto con los datos de comunicaciones relacionados. Como observó el ISR en su informe, actualmente hay mayores volúmenes de datos de comunicaciones disponibles sobre un individuo en relación con el contenido, ya que cada pieza de contenido está rodeada por múltiples piezas de datos de comunicaciones. Mientras que el contenido podría estar encriptado y, en cualquier caso, puede no revelar nada importante sobre el remitente o el destinatario, los datos de comunicaciones relacionados podrían revelar una gran cantidad de información personal, como las identidades y la ubicación geográfica del remitente y el destinatario y el equipo a través del cual se transmitió la comunicación. Además, cualquier intrusión ocasionada por la adquisición de datos de comunicaciones relacionados se magnificará cuando se obtengan en masa, ya que ahora son capaces de ser analizados e interrogados para pintar un cuadro íntimo de una persona a través del mapeo de redes sociales, seguimiento de ubicación, seguimiento de navegación en Internet, mapeo de patrones de comunicación y percepción de con quién interactuó una persona” (párrafo 342).

“Más importante aún, sin embargo, en *Weber y Saravia y Liberty y Otros* el Tribunal no abordó expresamente el hecho de que estaba tratando con vigilancia de una naturaleza y escala diferentes de las consideradas en casos anteriores. No obstante, la interceptación dirigida y la interceptación masiva son diferentes en varios aspectos importantes" (párrafo 343).

2. Principio de legalidad. Control de constitucionalidad. Reglamentación de los derechos. Control de legalidad. Declaración de inconstitucionalidad.

“Al evaluar si el Estado demandado actuó dentro de su margen de apreciación, el Tribunal necesitaría tener en cuenta una gama más amplia de criterios que las seis salvaguardias del caso *Weber*. Más específicamente, al abordar conjuntamente ´de acuerdo con la ley´ y ´necesidad´ como es el enfoque establecido en esta área (ver *Roman Zakharov*), el Tribunal examinará si el marco legal interno define claramente: 1. los motivos por los cuales se puede autorizar la interceptación masiva; 2. las circunstancias en las que se pueden interceptar las comunicaciones de un individuo; 3. el procedimiento a seguir para otorgar la autorización; 4. los procedimientos a seguir para seleccionar, examinar y usar el material interceptado; 5. las precauciones a tomar al comunicar el material a otras partes; 6. los límites sobre la duración de la interceptación, el almacenamiento del material interceptado y las circunstancias en las que dicho material debe ser borrado y destruido; 7. los procedimientos y modalidades para la supervisión por una autoridad independiente del cumplimiento de las salvaguardias anteriores y sus poderes para abordar el incumplimiento; 8. los procedimientos para la revisión independiente *ex post facto* de dicho cumplimiento y los poderes otorgados al órgano competente para abordar los casos de incumplimiento” (párrafo 361).

“[E]l Tribunal considera que la transmisión por un Estado contratante a Estados extranjeros u organizaciones internacionales de material obtenido por interceptación masiva debería limitarse a dicho material que haya sido recopilado y almacenado de manera compatible con el Convenio

y debería estar sujeta a ciertas salvaguardias adicionales específicas relativas a la transferencia en sí. En primer lugar, las circunstancias en las que puede tener lugar dicha transferencia deben estar establecidas claramente en el derecho interno. En segundo lugar, el Estado que transfiere debe asegurarse de que el Estado receptor, al manejar los datos, tenga en vigor salvaguardias capaces de prevenir abusos e interferencias desproporcionadas. En particular, el Estado receptor debe garantizar el almacenamiento seguro del material y restringir su divulgación posterior. Esto no significa necesariamente que el Estado receptor deba tener una protección comparable a la del Estado que transfiere; ni requiere necesariamente que se dé una garantía antes de cada transferencia. En tercer lugar, se necesitarán salvaguardias reforzadas cuando esté claro que se está transfiriendo material que requiere confidencialidad especial, como material periodístico confidencial. Finalmente, el Tribunal considera que la transferencia de material a socios de inteligencia extranjeros también debe estar sujeta a control independiente" (párrafo 362)

“En el momento relevante, la interceptación masiva tenía una base legal en el Capítulo I de RIPA. Además, el Tribunal está satisfecho de que dicho régimen perseguía los objetivos legítimos de proteger la seguridad nacional, prevenir el desorden y el crimen y proteger los derechos y libertades de otros. Por lo tanto, [...] queda por considerar si el derecho interno era accesible y contenía salvaguardias y garantías adecuadas y efectivas para cumplir con los requisitos de ´previsibilidad´ y ´necesidad en una sociedad democrática´” (párrafo 365).

“Las disposiciones legislativas relevantes que rigen la operación del régimen de interceptación masiva eran sin duda complejas; de hecho, la mayoría de los informes sobre los regímenes de vigilancia secreta del Reino Unido criticaron su falta de claridad. Sin embargo, esas disposiciones fueron aclaradas en el Código de Práctica de Interceptación de Comunicaciones (´el Código IC´) que lo acompañaba. El párrafo 6.4 del Código IC dejaba claro que se estaba llevando a cabo la interceptación masiva y proporcionaba más detalles sobre cómo operaba este régimen de vigilancia particular en la práctica. El Código IC es un documento público aprobado por ambas Cámaras del Parlamento, que es publicado por el Gobierno en línea y en versión impresa, y que debe ser tenido en cuenta tanto por las personas que ejercen funciones de interceptación como por los tribunales. Como consecuencia, este Tribunal ha aceptado que sus disposiciones pudieran tenerse en cuenta al evaluar la previsibilidad de RIPA (ver caso Kennedy). En consecuencia, el Tribunal aceptaría que el derecho interno era adecuadamente ´accesible´” (párrafo 366).

3. Control judicial. Auditoría. Principio de proporcionalidad. Acceso a la justicia. Derecho defensa. Legitimación. Recursos judiciales.

"En su jurisprudencia sobre la interceptación de comunicaciones en investigaciones penales, el Tribunal ha desarrollado los siguientes requisitos mínimos que deben establecerse en la ley para evitar abusos de poder: (i) la naturaleza de los delitos que pueden dar lugar a una orden de interceptación; (ii) una definición de las categorías de personas susceptibles de que se intercepten sus comunicaciones; (iii) un límite a la duración de la interceptación; (iv) el procedimiento a seguir para examinar, utilizar y almacenar los datos obtenidos; (v) las precauciones que deben tomarse al comunicar los datos a otras partes; y (vi) las circunstancias en las que los datos interceptados pueden o deben ser borrados o destruidos" (párrafo 335).

“En cuanto a la cuestión de si una interferencia era ´necesaria en una sociedad democrática´ en la consecución de un objetivo legítimo, el Tribunal ha reconocido que las autoridades nacionales gozan de un amplio margen de apreciación en la elección de los medios para alcanzar el objetivo legítimo de proteger la seguridad nacional (ver caso *Weber y Saravia*)” (párrafo 338).

“[E]ste margen [de apreciación] está sujeto a supervisión europea que abarca tanto la legislación como las decisiones que la aplican. En vista del riesgo de que un sistema de vigilancia secreta establecido para proteger la seguridad nacional (y otros intereses nacionales esenciales) pueda socavar o incluso destruir la democracia bajo el manto de defenderla, el Tribunal debe estar

convencido de que existen garantías adecuadas y efectivas contra el abuso. La evaluación depende de todas las circunstancias del caso, como la naturaleza, alcance y duración de las posibles medidas, los motivos requeridos para ordenarlas, las autoridades competentes para autorizarlas, llevarlas a cabo y supervisarlas, y el tipo de recurso previsto por la ley nacional. El Tribunal tiene que determinar si los procedimientos para supervisar la ordenación y la implementación de las medidas restrictivas son tales como para mantener la ´interferencia´ a lo que es ´necesario en una sociedad democrática´ (ver casos *Roman Zakharov*; ver también *Klass y Otros*; *Weber y Saravia*; y *Kennedy*)" (párrafo 339).

"[L]a interceptación masiva está generalmente dirigida a las comunicaciones internacionales (es decir, las comunicaciones que viajan físicamente a través de las fronteras estatales), y aunque la interceptación e incluso el examen de las comunicaciones de personas dentro del Estado vigilante podría no estar excluido, en muchos casos el propósito declarado de la interceptación masiva es monitorear las comunicaciones de personas fuera de la jurisdicción territorial del Estado, lo que no podría ser monitoreado por otras formas de vigilancia" (párrafo 344).

"[A]unque la interceptación masiva no se utiliza necesariamente para dirigirse a individuos específicos, evidentemente puede ser —y es— utilizada para este propósito. Sin embargo, cuando este es el caso, los dispositivos de los individuos objetivo no son monitoreados. Más bien, los individuos son ´objetivo´ mediante la aplicación de fuertes selectores (como sus direcciones de correo electrónico) a las comunicaciones interceptadas en masa por los servicios de inteligencia" (párrafo 346).

"[L]os Estados gozan de un amplio margen de apreciación en la decisión de qué tipo de régimen de interceptación es necesario para proteger la seguridad nacional, pero este margen de apreciación debe estar sujeto a supervisión europea en lo que respecta a la adecuación y efectividad de las garantías contra el abuso. La necesidad de tales garantías es particularmente grande donde, como en el presente caso, está en juego la protección de datos personales sometidos a procesamiento automático, no menos cuando estos datos son procesados para fines policiales. El grado de interferencia con los derechos de privacidad que tal procesamiento puede causar dependerá de las circunstancias del caso en particular. Sin embargo, el mero hecho de que el procesamiento pueda llevarse a cabo a gran escala aumenta el riesgo de abuso" (párrafo 347).

"El Tribunal es claro en que no es necesario que el derecho interno establezca de antemano todas las situaciones que podrían dar lugar a una orden de interceptación. Por el contrario, es imperativo que cuando un Estado está operando tal régimen, el derecho interno contenga reglas detalladas sobre cuándo las autoridades pueden recurrir a tales medidas. En particular, el derecho interno debe establecer con suficiente claridad los motivos sobre los cuales puede autorizarse la interceptación masiva y las circunstancias en las que pueden interceptarse las comunicaciones de un individuo" (párrafo 348).

"[E]l Tribunal ha indicado que en un contexto donde el poder del ejecutivo se ejerce en secreto, el riesgo de arbitrariedad es evidente. Por lo tanto, es esencial tener reglas claras y detalladas sobre medidas de vigilancia secretas, especialmente porque la tecnología disponible para su uso se está volviendo continuamente más sofisticada. El derecho interno debe ser lo suficientemente claro como para dar a los ciudadanos una indicación adecuada de las circunstancias y condiciones en las que las autoridades están facultadas para recurrir a tales medidas. Además, debido al riesgo de abuso intrínseco a cualquier sistema de vigilancia secreta, tales medidas deben basarse en una ley que sea particularmente precisa, especialmente porque la tecnología disponible para su uso se está volviendo continuamente más sofisticada" (párrafo 349).

"[E]l Tribunal considera que para minimizar el riesgo de que el poder de interceptación masiva sea abusado, el proceso debe estar sujeto a ´salvaguardias de principio a fin´, lo que significa que, a nivel nacional, se debe realizar una evaluación en cada etapa del proceso de la necesidad y

proporcionalidad de las medidas que se están tomando; que la interceptación masiva debe estar sujeta a autorización independiente al inicio, cuando se está definiendo el objeto y el alcance de la operación; y que la operación debe estar sujeta a supervisión y revisión independiente *ex post facto*" (párrafo 350).

“Cada etapa del proceso de interceptación masiva —incluida la autorización inicial y cualquier renovación posterior, la selección de portadores, la elección y aplicación de selectores y términos de búsqueda, y el uso, almacenamiento, transmisión posterior y eliminación del material interceptado— también debe estar sujeta a supervisión por una autoridad independiente y esa supervisión debe ser lo suficientemente robusta como para mantener la ´interferencia´ en lo que es ´necesario en una sociedad democrática´ (ver *Roman Zakharov*; ver también *Klass y Otros*; *Weber y Saravia y Kennedy*, respectivamente). En particular, el órgano supervisor debe estar en posición de evaluar la necesidad y proporcionalidad de la acción que se está tomando, teniendo debidamente en cuenta el correspondiente nivel de intrusión en los derechos del Convenio de las personas que probablemente se verán afectadas. Para facilitar esta supervisión, los servicios de inteligencia deben mantener registros detallados en cada etapa del proceso” (párrafo 356).

“[D]ebe estar disponible un recurso efectivo para cualquiera que sospeche que sus comunicaciones han sido interceptadas por los servicios de inteligencia, ya sea para impugnar la legalidad de la supuesta interceptación o la conformidad con el Convenio del régimen de interceptación. En el contexto de la interceptación dirigida, el Tribunal ha encontrado repetidamente que la notificación posterior de las medidas de vigilancia es un factor relevante para evaluar la efectividad de los recursos ante los tribunales y, por lo tanto, la existencia de salvaguardias efectivas contra el abuso de los poderes de vigilancia. Sin embargo, ha reconocido que la notificación no es necesaria si el sistema de recursos internos permite a cualquier persona que sospeche que sus comunicaciones están siendo o han sido interceptadas aplicar a los tribunales; en otras palabras, donde la jurisdicción de los tribunales no depende de la notificación al sujeto de la interceptación de que ha habido una interceptación de sus comunicaciones (ver *Roman Zakharov y Kennedy*)" (párrafo 357).

“El Tribunal considera que un recurso que no depende de la notificación al sujeto de la interceptación también podría ser un recurso efectivo en el contexto de la interceptación masiva; de hecho, dependiendo de las circunstancias, incluso podría ofrecer mejores garantías de un procedimiento adecuado que un sistema basado en la notificación. Independientemente de si el material fue adquirido a través de interceptación dirigida o masiva, la existencia de una excepción de seguridad nacional podría privar a un requisito de notificación de cualquier efecto práctico real. La probabilidad de que un requisito de notificación tenga poco o ningún efecto práctico será más aguda en el contexto de la interceptación masiva, ya que dicha vigilancia puede ser utilizada para fines de recopilación de inteligencia extranjera y, en su mayor parte, apuntará a las comunicaciones de personas fuera de la jurisdicción territorial del Estado. Por lo tanto, incluso si se conoce la identidad de un objetivo, las autoridades pueden no estar al tanto de su ubicación” (párrafo 358).

“Las facultades y garantías procesales que posee una autoridad son relevantes para determinar si un recurso es efectivo. Por lo tanto, en ausencia de un requisito de notificación, es imperativo que el recurso sea ante un organismo que, aunque no necesariamente judicial, sea independiente del ejecutivo y garantice la equidad del procedimiento, ofreciendo, en la medida de lo posible, un proceso contradictorio. Las decisiones de dicha autoridad deberán ser razonadas y legalmente vinculantes con respecto, entre otras cosas, al cese de la interceptación ilegal y la destrucción del material interceptado obtenido y/o almacenado ilegalmente (ver, *mutatis mutandis, Segerstedt-Wiberg y Otros v. Suecia* y también *Leander* donde la falta de poder para dictar una decisión legalmente vinculante constituía una debilidad principal en el control ofrecido)" (párrafo 359).

4. Protección de datos personales. Derecho a la intimidad. Consentimiento informado. Libertad de expresión. Derecho a la información. Datos biométricos. Derecho al honor.

“A pesar de ser uno de los seis criterios de *Weber*, hasta la fecha el Tribunal aún no ha proporcionado orientación específica con respecto a las precauciones a tomar al comunicar material interceptado a otras partes. Sin embargo, ahora está claro que algunos Estados comparten regularmente material con sus socios de inteligencia e incluso, en algunos casos, permiten que esos socios de inteligencia tengan acceso directo a sus propios sistemas. En consecuencia, el Tribunal considera que la transmisión por un Estado contratante a Estados extranjeros u organizaciones internacionales de material obtenido por interceptación masiva debería limitarse a dicho material que haya sido recopilado y almacenado de manera compatible con el Convenio y debería estar sujeta a ciertas salvaguardias adicionales específicas relativas a la transferencia misma” (párrafo 353).

“Teniendo en cuenta las características de la interceptación masiva, el gran número de selectores empleados y la necesidad inherente de flexibilidad en la elección de selectores, que en la práctica pueden expresarse como combinaciones técnicas de números o letras, el Tribunal aceptaría que la inclusión de todos los selectores en la autorización puede no ser factible en la práctica. Sin embargo, dado que la elección de selectores y términos de búsqueda determina qué comunicaciones serán elegibles para examen por un analista, la autorización debería, como mínimo, identificar los tipos o categorías de selectores que se utilizarán” (párrafo 354).

“[D]eberían existir salvaguardias reforzadas cuando se emplean selectores fuertes vinculados a individuos identificables por los servicios de inteligencia. El uso de cada uno de estos selectores debe estar justificado —con respecto a los principios de necesidad y proporcionalidad— por los servicios de inteligencia y esa justificación debe ser registrada escrupulosamente y estar sujeta a un proceso de autorización interna previa que proporcione una verificación separada y objetiva de si la justificación se ajusta a los principios antes mencionados" (párrafo 355).

“[E]l Tribunal no está convencido de que la adquisición de datos de comunicaciones relacionados a través de la interceptación masiva sea necesariamente menos intrusiva que la adquisición de contenido. Por lo tanto, considera que la interceptación, retención y búsqueda de datos de comunicaciones relacionados deberían analizarse por referencia a las mismas salvaguardias aplicables al contenido” (párrafo 363).

“[M]ientras que la interceptación de datos de comunicaciones relacionados normalmente se autorizará al mismo tiempo que se autoriza la interceptación de contenido, una vez obtenidos pueden ser tratados de manera diferente por los servicios de inteligencia. En vista del carácter diferente de los datos de comunicaciones relacionados y las diferentes formas en que son utilizados por los servicios de inteligencia, siempre que las salvaguardias antes mencionadas estén en su lugar, el Tribunal es de la opinión que las disposiciones legales que rigen su tratamiento pueden no necesariamente tener que ser idénticas en todos los aspectos a las que rigen el tratamiento del contenido" (párrafo 364).

“Cuando la intención de los servicios de inteligencia es acceder a material periodístico confidencial, por ejemplo, a través del uso deliberado de un selector fuerte conectado a un periodista, o cuando, como resultado de la elección de tales selectores fuertes, existe una alta probabilidad de que dicho material sea seleccionado para examen, el Tribunal considera que la interferencia será conmensurable con la ocasionada por el registro del domicilio o lugar de trabajo de un periodista; independientemente de si la intención de los servicios de inteligencia es identificar una fuente o no, el uso de selectores o términos de búsqueda conectados a un periodista muy probablemente resultaría en la adquisición de cantidades significativas de material periodístico confidencial que podría socavar la protección de las fuentes en una medida aún mayor que una orden para revelar una fuente (ver *Roemen* y *Schmit*). Por lo tanto, el Tribunal

considera que antes de que los servicios de inteligencia utilicen selectores o términos de búsqueda que se sabe están conectados a un periodista, o que harían altamente probable la selección de material periodístico confidencial para examen, los selectores o términos de búsqueda deben haber sido autorizados por un juez u otro organismo independiente e imparcial de toma de decisiones investido con el poder de determinar si son ´justificados por un requisito primordial de interés público´ y, en particular, si una medida menos intrusiva podría haber sido suficiente para servir al interés público primordial (ver *Sanoma Uitgevers B.V*.) (párrafo 448).

"Incluso cuando no hay intención de acceder a material periodístico confidencial, y los selectores y términos de búsqueda utilizados no son tales que hagan altamente probable la selección de material periodístico confidencial para examen, todavía existirá un riesgo de que dicho material pueda ser interceptado, e incluso examinado, como un ´efecto secundario´ de una operación de interceptación masiva. En opinión del Tribunal, esta situación es materialmente diferente de la vigilancia dirigida de un periodista a través de los regímenes de la sección 8(1) o la sección 8(4). Como la interceptación de cualquier comunicación periodística sería involuntaria, el grado de interferencia con las comunicaciones periodísticas y/o fuentes no podría predecirse al inicio. En consecuencia, no sería posible en la etapa de autorización que un juez u otro organismo independiente evalúe si dicha interferencia estuviera ´justificada por un requisito primordial de interés público´ y, en particular, si una medida menos intrusiva podría haber sido suficiente para servir al interés público primordial" (párrafo 448).

"En *Weber y Saravia*, el Tribunal sostuvo que la interferencia con la libertad de expresión causada por el monitoreo estratégico no podía caracterizarse como particularmente grave ya que no estaba dirigida a monitorear periodistas y las autoridades sabrían solo cuando examinaran las telecomunicaciones interceptadas, si es que lo hacían, que se habían monitoreado las comunicaciones de un periodista (ver *Weber y Saravia*). Por lo tanto, aceptó que la interceptación inicial, sin examen del material interceptado, no constituía una interferencia grave con el artículo 10 del Convenio. Sin embargo, como el Tribunal ya ha observado, en la actual era cada vez más digital, las capacidades tecnológicas han aumentado enormemente el volumen de comunicaciones que atraviesan la Internet global, y como consecuencia la vigilancia que no está dirigida directamente a individuos tiene la capacidad de tener un alcance muy amplio, tanto dentro como fuera del territorio del Estado que realiza la vigilancia. Como el examen de las comunicaciones de un periodista o datos de comunicaciones relacionados por un analista sería capaz de llevar a la identificación de una fuente, el Tribunal considera imperativo que el derecho interno contenga salvaguardias robustas con respecto al almacenamiento, examen, uso, transmisión posterior y destrucción de dicho material confidencial. Además, incluso si una comunicación periodística o datos de comunicaciones relacionados no han sido seleccionados para examen a través del uso deliberado de un selector o término de búsqueda que se sabe está conectado a un periodista, si y cuando se haga evidente que la comunicación o datos de comunicaciones relacionados contienen material periodístico confidencial, su almacenamiento y examen continuos por un analista solo deberían ser posibles si están autorizados por un juez u otro organismo independiente e imparcial de toma de decisiones investido con el poder de determinar si el almacenamiento y examen continuos están ´justificados por un requisito primordial de interés público´" (párrafo 449).

"El Tribunal acepta que un recurso que no depende de la notificación al sujeto de la interceptación también podría ser un recurso efectivo en el contexto de la interceptación masiva; de hecho, dependiendo de las circunstancias, incluso podría ofrecer mejores garantías de un procedimiento adecuado que un sistema basado en la notificación. Independientemente de si el material fue adquirido a través de interceptación dirigida o masiva, la existencia de una excepción de seguridad nacional podría privar a un requisito de notificación de cualquier efecto práctico real. La probabilidad de que un requisito de notificación tenga poco o ningún efecto práctico será más aguda en el contexto de la interceptación masiva, ya que dicha vigilancia puede ser utilizada para

fines de recopilación de inteligencia extranjera y, en su mayor parte, apuntará a las comunicaciones de personas fuera de la jurisdicción territorial del Estado. Por lo tanto, incluso si se conoce la identidad de un objetivo, las autoridades pueden no estar al tanto de su ubicación" (párrafo 450).

5. Control de legalidad. Auditoría. Sistema informático. Política criminal. Control judicial. Principio de legalidad.

"A pesar de ser uno de los seis criterios de[l caso] Weber, hasta la fecha el Tribunal aún no ha proporcionado orientación específica con respecto a las precauciones a tomar al comunicar material interceptado a otras partes. Sin embargo, ahora está claro que algunos Estados comparten regularmente material con sus socios de inteligencia e incluso, en algunos casos, permiten que esos socios de inteligencia tengan acceso directo a sus propios sistemas. En consecuencia, el Tribunal considera que la transmisión por un Estado contratante a Estados extranjeros u organizaciones internacionales de material obtenido por interceptación masiva debería limitarse a dicho material que haya sido recopilado y almacenado de manera compatible con el Convenio y debería estar sujeta a ciertas salvaguardias adicionales específicas relativas a la transferencia misma. En primer lugar, las circunstancias en las que puede tener lugar dicha transferencia deben estar establecidas claramente en el derecho interno. En segundo lugar, el Estado que transfiere debe asegurarse de que el Estado receptor, al manejar los datos, tenga en vigor salvaguardias capaces de prevenir abusos e interferencias desproporcionadas. En particular, el Estado receptor debe garantizar el almacenamiento seguro del material y restringir su divulgación posterior. Esto no significa necesariamente que el Estado receptor deba tener una protección comparable a la del Estado que transfiere; ni requiere necesariamente que se dé una garantía antes de cada transferencia. En tercer lugar, se necesitarán salvaguardias reforzadas cuando sea claro que se está transfiriendo material que requiere confidencialidad especial, como material periodístico confidencial. Finalmente, el Tribunal considera que la transferencia de material a socios de inteligencia extranjeros también debe estar sujeta a control independiente" (párrafo 362).

"El Acuerdo de Inteligencia de Comunicaciones Británico-Estadounidense del 5 de marzo de 1946 permitía específicamente el intercambio de material entre los Estados Unidos y el Reino Unido. Sin embargo, los detalles de los arreglos internos (o ´bajo la línea de flotación´) de los servicios de inteligencia solo se revelaron durante los procedimientos de *Liberty*. Esta nueva información se incorporó posteriormente al Capítulo 12 del Código IC que, como ya se ha señalado, era un documento público, sujeto a la aprobación de ambas Cámaras del Parlamento, y que debía ser tenido en cuenta tanto por quienes ejercían funciones de interceptación como por los tribunales y tribunales. El Tribunal ha aceptado que las disposiciones del Código IC podrían tenerse en cuenta al evaluar la previsibilidad del régimen RIPA (ver Kennedy) y lo mismo debe ser necesariamente cierto para el régimen de intercambio de inteligencia" (párrafo 498).

"[E]l Tribunal considera que el régimen para solicitar y recibir inteligencia de Estados no contratantes tenía una base clara en el derecho interno y, tras la enmienda al Código IC, ese derecho era adecuadamente accesible. Como indudablemente perseguía los objetivos legítimos de proteger la seguridad nacional, prevenir el desorden y el crimen y proteger los derechos y libertades de otros, el Tribunal ahora —en línea con su metodología habitual— evaluará, conjuntamente, la previsibilidad y necesidad del régimen de intercambio de inteligencia" (párrafo 499).

"El Capítulo 12 del Código IC sigue el mismo enfoque que el adoptado por la legislación nacional con respecto a la interceptación masiva. Según el Capítulo 12, los servicios de inteligencia solo podían hacer una solicitud a un gobierno extranjero de comunicaciones interceptadas no analizadas y/o datos de comunicaciones asociados si ya se había emitido una orden de interceptación relevante bajo RIPA por el Secretario de Estado, la asistencia del gobierno

extranjero era necesaria para obtener las comunicaciones particulares porque no podían obtenerse bajo la orden existente (ver párrafo 12.2 del Código IC en el párrafo 116 arriba), y era necesario y proporcionado para la agencia interceptora obtener esas comunicaciones. Para estos propósitos, una orden de interceptación RIPA relevante significaba ya sea una orden de la sección 8(1) en relación con el tema en cuestión; una orden de la sección 8(4) y un certificado acompañante que incluía una o más ´descripciones de material interceptado´ cubriendo las comunicaciones del sujeto; o, cuando se sabía que el sujeto estaba dentro de las Islas Británicas, una orden de la sección 8(4) y un certificado acompañante que incluía una o más ´descripciones de material interceptado´ cubriendo sus comunicaciones, junto con una modificación apropiada de la sección 16(3)" (párrafo 500).

“Cuando existían circunstancias excepcionales, se podía hacer una solicitud de comunicaciones en ausencia de una orden de interceptación RIPA relevante solo si no equivalía a una elusión deliberada de RIPA o de otra manera frustraba sus objetivos (por ejemplo, porque no era técnicamente factible obtener las comunicaciones a través de la interceptación RIPA), y era necesario y proporcionado para la agencia interceptora obtener esas comunicaciones. En tal caso, la solicitud tenía que ser considerada y decidida por el secretario de Estado personalmente, y, de acuerdo con el Código IC revisado, notificada al Comisionado IC. Según la información revelada durante los procedimientos de *Liberty*, y confirmada en las presentaciones del Gobierno ante la Sala y la Gran Sala, nunca se había hecho una solicitud de material interceptado en ausencia de una orden RIPA existente (párrafo 501)”.

“[E]l Tribunal considera que el derecho interno estableció reglas legales claras que dan a los ciudadanos una indicación adecuada de las circunstancias y condiciones en las que las autoridades podían solicitar material interceptado de un Estado extranjero” (párrafo 502).

“Cuando ya existía una orden relevante de la sección 8(1) o de la sección 8(4), esa orden habría sido autorizada por el secretario de Estado. Más específicamente, parecería del párrafo 12.5 del Código IC, leído junto con la nota al pie que lo acompaña, que cuando una solicitud se basaba en una orden existente, esa solicitud se haría a, desde o sobre selectores específicos (es decir, relacionados con un individuo o individuos específicos) y el secretario de Estado ya habría aprobado la solicitud de las comunicaciones de esos individuos. Mientras que, en circunstancias excepcionales, se podía hacer una solicitud en ausencia de una orden relevante, el secretario de Estado personalmente tenía que aprobar la solicitud y, si se basaba en selectores específicos, él o ella personalmente tenía que considerar y aprobar el examen de esas comunicaciones por referencia a tales factores” (párrafo 503).

“Como la legislación nacional siguió, con respecto a tales solicitudes de intercambio de inteligencia, el mismo enfoque que en la interceptación masiva, y como la ley nacional explícitamente preveía que no debería haber elusión, no hay necesidad de que el Tribunal examine por separado el procedimiento de autorización” (párrafo 504).

“En cuanto a las salvaguardias para el examen, uso, almacenamiento, transmisión posterior, borrado y destrucción del material interceptado solicitado, quedaba claro del párrafo 12.6 del Código IC que el contenido interceptado o los datos de comunicaciones relacionados obtenidos por los servicios de inteligencia del Reino Unido de otro Estado, que se identificaban a sí mismos como producto de intercepción, tenían que estar sujetos a las mismas reglas y salvaguardias internas que se aplicaban a las mismas categorías de contenido o datos cuando eran obtenidos directamente por las agencias interceptoras como resultado de la interceptación bajo RIPA. En consecuencia, las salvaguardias en las secciones 15 y 16 de RIPA, complementadas por el Código IC, se aplicaban igualmente a las comunicaciones interceptadas y los datos de comunicaciones obtenidos de servicios de inteligencia extranjeros, siempre que el material ´se identificara a sí mismo como producto de intercepción´” (párrafo 505).

"El Tribunal ha examinado las salvaguardias de las secciones 15 y 16 con respecto al régimen de interceptación masiva y estaba satisfecho de que los procedimientos para almacenar, acceder, examinar y usar el material obtenido; para comunicar el material a otras partes; y para el borrado y destrucción del material obtenido eran suficientemente claros y proporcionaban una protección adecuada contra el abuso. A la luz de las conclusiones del Tribunal en el párrafo 498 arriba, observa que el párrafo 12.6 del Código IC no extiende las salvaguardias de las secciones 15 y 16 de RIPA, complementadas por el Código IC, a todo el material recibido de servicios de inteligencia extranjeros que pudiera ser producto de intercepción, limitando estas salvaguardias solo al material que se identificara a sí mismo como tal; sin embargo, el Tribunal no considera que este hecho por sí solo sea fatal para la compatibilidad con el artículo 8 del régimen de intercambio de inteligencia" (párrafo 506).

"En el contexto del régimen de la sección 8(4), el Tribunal tenía preocupaciones sobre la exención de los datos de comunicaciones relacionados de la salvaguardia de la sección 16. Sin embargo, bajo el régimen de la sección 8(4) el Estado podía interceptar, almacenar y buscar todos los paquetes de comunicaciones que viajaban a través de ciertos portadores. La exención general de los datos de comunicaciones relacionados de la salvaguardia de la sección 16 significaba, por lo tanto, que todos estos datos, independientemente de si eran de algún interés de inteligencia, podían ser buscados por los servicios de inteligencia aparentemente sin restricción. Bajo el Capítulo 12 del Código IC, por otro lado, el contenido y los datos de comunicaciones relacionados no eran solicitados por los servicios de inteligencia en masa. El párrafo 12.5 del Código IC, junto con su nota al pie, indicaba que cuando una solicitud se basaba en una orden existente, esa solicitud se haría a, desde o sobre selectores específicos (es decir, individuos especificados) y el secretario de Estado ya habría aprobado la solicitud de las comunicaciones de esos individuos. Mientras que en circunstancias excepcionales se podía hacer una solicitud en ausencia de una orden, el secretario de Estado personalmente tenía que aprobar la solicitud y, si se basaba en selectores específicos, él o ella personalmente tenía que considerar y aprobar el examen de esas comunicaciones por referencia a tales factores. Si la solicitud no era para selectores específicos, cualquier comunicación obtenida posteriormente no podía ser examinada de acuerdo con un factor referible a una persona conocida por estar en las Islas Británicas a menos que el secretario de Estado hubiera aprobado el examen de esas comunicaciones. En otras palabras, los servicios de inteligencia solicitaban inteligencia relacionada con un individuo para el cual el secretario de Estado ya había considerado la necesidad y proporcionalidad de obtener sus comunicaciones; o la salvaguardia de la sección 16 era aplicable al material obtenido. Como no se ha hecho ninguna solicitud sin una orden, parecería que, hasta la fecha, todas las solicitudes han caído en la primera categoría" (párrafo 507).

"[E]l Tribunal considera que el Reino Unido tenía en vigor salvaguardias adecuadas para el examen, uso y almacenamiento del contenido y los datos de comunicaciones recibidos de socios de inteligencia; para la transmisión posterior de este material; y para su borrado y destrucción" (párrafo 508).

"[E]l Tribunal observa que una capa adicional de protección fue proporcionada por el Comisionado IC y el IPT. El Comisionado IC tenía supervisión del régimen de intercambio de inteligencia: el párrafo 12.7 del Código IC requería que se le notificara de todas las solicitudes hechas en ausencia de una orden, y ya supervisaba la concesión de órdenes y el almacenamiento de material por los servicios de inteligencia" (párrafo 509).

"Además de la supervisión del Comisionado IC, el IPT proporcionó revisión ex post facto del régimen de intercambio de inteligencia. Como se puede ver en los procedimientos de *Liberty*, estaba abierto a cualquiera que deseara hacer una queja específica o general sobre el régimen de intercambio de inteligencia quejarse al IPT; y, en respuesta, el IPT podía examinar tanto los

arreglos ´sobre la línea de flotación´ como los ´bajo la línea de flotación´ para evaluar la conformidad con el Convenio del régimen" (párrafo 510).

"[E]l Tribunal considera que el régimen para solicitar y recibir material interceptado era compatible con el artículo 8 del Convenio. Existían reglas claras y detalladas que daban a los ciudadanos una indicación adecuada de las circunstancias y condiciones en las que las autoridades estaban facultadas para hacer una solicitud a un servicio de inteligencia extranjero; el derecho interno contenía garantías efectivas contra el uso de tales solicitudes para eludir el derecho interno y/o las obligaciones del Reino Unido bajo el Convenio; el Reino Unido tenía en vigor salvaguardias adecuadas para el examen, uso, almacenamiento, transmisión posterior, borrado y destrucción del material; y el régimen estaba sujeto a supervisión independiente por el Comisionado IC y había una posibilidad de revisión *ex post facto* por el IPT" (párrafo 511).

"Los demandantes en el tercero de los casos unidos también se quejaron de que el régimen de intercambio de inteligencia había violado sus derechos bajo el artículo 10 del Convenio. En la medida en que esa queja se relacionaba con sus actividades como ONGs, la Sala la declaró inadmisible por no agotamiento de los recursos internos ya que los demandantes la habían planteado demasiado tarde en los procedimientos internos para que fuera considerada. Este aspecto de la queja está, por lo tanto, fuera del alcance del examen de la Gran Sala" (párrafo 513)

"En la fecha del examen del caso por parte de la Sala, el Gobierno del Reino Unido estaba en proceso de reemplazar el marco legal existente para llevar a cabo la vigilancia secreta con la nueva IPA. Las disposiciones en la nueva legislación que rigen la retención de datos de comunicaciones por parte de los CSP estaban sujetas a un desafío legal interno por *Liberty*. En el curso de esos procedimientos, el Gobierno concedió que la disposición relevante era inconsistente con los requisitos del derecho de la UE. En consecuencia, el Tribunal Superior encontró que la Parte 4 era incompatible con los derechos fundamentales en el derecho de la UE ya que, en el área de la justicia penal, el acceso a los datos retenidos no se limitaba al propósito de combatir el ´crimen grave´; ni estaba sujeto a revisión previa por un tribunal o un organismo administrativo independiente (párrafo 518).

"En vista tanto de la primacía del derecho de la UE sobre el derecho del Reino Unido, como de la concesión del Gobierno en los procedimientos internos de que las disposiciones de IPA que rigen la retención de datos de comunicaciones por parte de los CSP eran incompatibles con el derecho de la UE, la Sala consideró ´claro´ que el derecho interno requería que cualquier régimen que permitiera a las autoridades acceder a datos retenidos por los CSP debería limitar el acceso al propósito de combatir el ´crimen grave´, y que el acceso debería estar sujeto a revisión previa por un tribunal o un organismo administrativo independiente. Como el régimen predecesor sufría de las mismas ´fallas´ que su sucesor, la Sala encontró que no podía estar de acuerdo con la ley en el sentido del artículo 8 del Convenio" (párrafo 519).

"[E]l Tribunal considera que en el presente caso hubo una violación del artículo 8 del Convenio debido al hecho de que la operación del régimen bajo el Capítulo II de RIPA no estaba ´de acuerdo con la ley´" (párrafo 522).

Opinión conjunta parcialmente concurrente de los jueces Lemmens, Vehabović y Bošnjak

Crítica a la falta de énfasis en la importancia de la privacidad

"[V]ale la pena recordar que la privacidad es una precondición fundamental para una variedad de intereses individuales fundamentales, pero también para la existencia de una sociedad democrática. Es esencial para el bienestar, la autonomía, el autodesarrollo y la capacidad de una persona para entablar relaciones significativas con otros. También es una precondición necesaria para el disfrute de los derechos civiles y, en consecuencia, para el estatus de una persona como miembro libre e igual de una sociedad democrática. Las intromisiones en la privacidad no solo

disminuyen la autonomía individual y la salud mental y física, sino que también inhiben el autogobierno democrático" (párrafo 3).

"[L]a privacidad es importante para la salud mental y física de una persona. El mero sentimiento de estar constantemente siendo observado y evaluado por otros puede tener efectos graves en el bienestar mental y físico de uno. Hace que los individuos internalicen demasiado su comportamiento social, de modo que se sienten culpables o avergonzados por cualquier sentimiento o pensamiento, deseo o práctica que no quisieran expresar públicamente. Tales tensiones entre las demandas de su vida interior y las presiones de la autopresentación pueden llevar a graves problemas de salud" (párrafo 4).

"[L]a observación externa y las presiones sobre la autopresentación pueden obstaculizar ´la promoción de la libertad, la autonomía, la individualidad, las relaciones humanas y el fomento de la existencia de una sociedad libre´. La vigilancia es inhibidora porque disminuye la medida en que podemos relacionarnos espontánea y sinceramente con otras personas y participar en ciertas actividades. La falta de privacidad tendría un efecto paralizante en nuestra vida interior, nuestras relaciones y, en última instancia, nuestra autonomía. ´Así se perderá...el núcleo personal interno que es la fuente de crítica de la convención, de creatividad, rebelión y renovación´" (párrafo 5).

"[L]a privacidad es esencial para el autogobierno democrático. La vigilancia masiva ejerce presiones internas y externas para conformarse, haciendo que los individuos sean sumisos y deferentes. Para evitar la opresión absoluta y darse el barniz de legitimidad, existe un peligro inherente de que el Estado utilice la vigilancia para asegurar el cumplimiento y el conformismo [...]" (párrafo 6).

"Al asegurar un ámbito para la actividad no observada, la privacidad fomenta y alienta la autonomía moral de los ciudadanos, un requisito central del autogobierno en las democracias. Solo los seres autónomos pueden verdaderamente gobernarse a sí mismos y solo los seres autónomos pueden verdaderamente disfrutar de todos los derechos civiles, como el derecho al voto, la libertad de asociación y la participación en la sociedad civil, las libertades de pensamiento y conciencia, de expresión y de religión, que son esenciales para el autogobierno. No se puede decir que disfrutemos plenamente de las libertades que estos derechos supuestamente nos otorgan si nuestra libertad interior está comprometida" (párrafo 7).

"Pero la vigilancia no solo ejerce presiones internas sobre la libertad. En la medida en que los ciudadanos conservan su autonomía, también ejerce presiones externas sobre su libertad para ejercer sus derechos civiles. Así como vivir bajo un control social constante nos hace menos propensos a actuar de acuerdo con nuestros sentimientos y pensamientos por miedo al ostracismo, vivir bajo vigilancia gubernamental constante puede hacer que los ciudadanos sean un poco más cautelosos al involucrarse con sus convicciones políticas, un poco menos propensos a asociarse libremente, un poco menos propensos a hablar libremente, un poco menos propensos a disentir, un poco menos propensos a postularse para un cargo público. El efecto agregado de inhibiciones a menudo meramente marginales puede ahogar lo que una vez fue una sociedad libre, especialmente a medida que las personas crecen en un ambiente de mayor conformismo y cobardía moral. El juez de la Corte Suprema de EE. UU. William O. Douglas, escribiendo la disidencia en *Osborn v. United States*, describe de manera impresionante la amenaza que la vigilancia masiva representa para nuestras libertades democráticas: ´... Puede llegar el momento en que nadie pueda estar seguro de si sus palabras están siendo grabadas para su uso en algún momento futuro; cuando todos teman que sus pensamientos más secretos ya no sean suyos, sino que pertenezcan al Gobierno; cuando las conversaciones más confidenciales e íntimas estén siempre abiertas a oídos ansiosos y curiosos. Cuando llegue ese momento, la privacidad y con ella la libertad habrán desaparecido. Si la privacidad de un hombre puede ser invadida a voluntad, ¿quién puede decir que es libre? Si cada una de sus palabras es registrada y evaluada, o si teme que cada palabra pueda serlo, ¿quién puede decir que disfruta de la libertad de expresión? Si se

conoce y registra cada una de sus asociaciones, si se hurtan las conversaciones con sus asociados, ¿quién puede decir que disfruta de la libertad de asociación? Cuando se den tales condiciones, nuestros ciudadanos tendrán miedo de expresar cualquier pensamiento que no sea el más seguro y ortodoxo; miedo de asociarse con cualquiera que no sea la gente más aceptable. La libertad tal como la prevé la Constitución habrá desaparecido´" (párrafo 8).

“[E]l desarrollo de nuevas tecnologías que permiten la vigilancia masiva y un uso más eficaz de la información recopilada ha aumentado las amenazas a la privacidad, así como el riesgo de abuso de los datos personales. No es nuestra intención afirmar que estas amenazas y riesgos ya se han materializado a gran escala o que han provocado las consecuencias discutidas anteriormente. Sin embargo, uno debería ser consciente de su existencia al diseñar un sistema capaz de prevenir, detectar y sancionar cualquier abuso que pueda ocurrir" (párrafo 9).

“[E]stas consideraciones deberían haber llevado al Tribunal a conceder un peso significativamente mayor a la vida privada en general, y a la confidencialidad de la correspondencia en particular, a la hora de sopesarlas en la balanza frente a los intereses legítimos del Estado demandado en el funcionamiento de su sistema de interceptación masiva. En consecuencia, la Gran Sala debería haber (a) identificado con precisión y atribuido el peso adecuado a las injerencias en la vida privada y la correspondencia; (b) introducido salvaguardias mínimas claras capaces de proteger a las personas contra injerencias arbitrarias o excesivas; y en consecuencia (c) evaluado el régimen de interceptación masiva impugnado de una manera más estricta” (párrafo 10).

Opinión parcialmente concurrente y parcialmente disidente del juez Pinto de Alburquerque

Cuestionamiento de la metodología del tribunal al evaluar la interceptación masiva

“El enfoque metodológico del Tribunal en este caso es lamentable, por dos razones principales. En primer lugar, el Tribunal estaba dispuesto a decidir un caso de esta importancia 'sobre la base de información limitada sobre la manera en que operan esos regímenes [de interceptación masiva de los Estados contratantes]'. Por ejemplo, el Gobierno no indicó el número o el grado de precisión de los selectores que habían utilizado, el número de portadores interceptados o cómo exactamente se seleccionaron esos portadores, o el tipo de informes de inteligencia que se estaban generando con respecto a los datos de comunicaciones relacionados, y sin embargo el Tribunal no insistió en obtener esa información crucial. El Tribunal de Poderes de Investigación (IPT) examinó los arreglos 'por debajo de la línea de flotación', el Comisionado de Interceptación de Comunicaciones (*IC Commissioner*) tuvo acceso a 'material cerrado' e incluso el Revisor Independiente de la legislación sobre Terrorismo examinó una 'gran cantidad de material cerrado', pero el Tribunal no lo hizo, y no pudo hacerlo. El Tribunal carecía evidentemente del material detallado necesario para hacer un análisis y evaluación estructural completos de la interceptación masiva en el Reino Unido. Es decepcionante que la máxima sensibilidad del tema de esta sentencia, que fue repetidamente subrayada por el Tribunal, solo sirviera para insistir en la necesidad de 'efectividad' y 'flexibilidad' del sistema de interceptación masiva, pero no para recopilar toda la evidencia relevante necesaria para una sentencia del Tribunal basada en hechos. Esta restricción autoimpuesta del poder del Tribunal para recopilar evidencia demuestra que los jueces de Estrasburgo no consideran al Tribunal como un verdadero órgano judicial, con el poder de ordenar a las partes que le proporcionen acceso ilimitado e incondicional a la evidencia relevante para el tema del caso. Como consecuencia, el Tribunal hizo algunas 'conjeturas educadas' sobre el probable grado de interferencia con los derechos de un individuo en diferentes etapas del proceso de interceptación. El problema de desarrollar estándares regulatorios sobre la base de tales 'conjeturas educadas' es que refleja las suposiciones y sesgos del regulador. Y son claros en el presente caso. El caso del Gobierno se reduce a una simple proposición que es 'confíen en nosotros'. La mayoría estaba dispuesta a aceptar esta proposición, con el riesgo de errar por el lado de la sobrecolección de inteligencia. Yo no lo estoy. Como lo expresó la Junta de Revisión

Presidencial de los Estados Unidos, 'los estadounidenses no deben cometer el error de confiar en los funcionarios'. Yo diría lo mismo para los europeos" (párrafo 4).

"En segundo lugar, la limitación evidencial y de adjudicación autoimpuesta mencionada anteriormente lleva al Tribunal a asumir la inevitabilidad de la interceptación masiva y, más aún, la de un régimen de interceptación general, no dirigido y sin sospecha, como alegaron el Estado demandado y los terceros tanto en el presente caso como en [el caso] *Centrum för rättvisa v. Suecia*. Con un razonamiento circular, el Gobierno afirmó que la interceptación masiva era incompatible con un requisito de sospecha razonable, porque era, por definición, no dirigida, y era no dirigida porque no requería sospecha razonable. El Tribunal siguió esta línea y lo expresó en términos axiomáticos: 'el requisito de 'sospecha razonable', que se puede encontrar en la jurisprudencia del Tribunal sobre interceptación dirigida en el contexto de investigaciones penales, es menos pertinente en el contexto de interceptación masiva, cuyo propósito es en principio preventivo, más que para la investigación de un objetivo específico y/o un delito penal identificable'.

De este nuevo paradigma se desprende que el Tribunal se ha apartado de la jurisprudencia establecida según la cual 'no considera que haya ningún motivo para aplicar diferentes principios relativos a la accesibilidad y claridad de las normas que rigen la interceptación de comunicaciones individuales, por un lado, y programas de vigilancia más generales, por otro'" (párrafo 5).

Las salvaguardas establecidas por la mayoría son insuficientes

"De este razonamiento fácticamente infundado, el Tribunal extrajo dos conclusiones legales para 'el enfoque a seguir en casos de interceptación masiva': la ley nacional no tiene que identificar la naturaleza de los delitos que pueden dar lugar a una orden de interceptación y las categorías de personas cuyas comunicaciones pueden ser interceptadas, y no se necesita ningún requisito de sospecha razonable para fundamentar dicha orden de interceptación. Según la lógica del Tribunal, dado que 'el propósito de [la interceptación masiva] es en principio preventivo, más que para la investigación de un objetivo específico y/o un delito penal identificable', ninguna de las dos salvaguardias anteriores se requiere en la ley nacional, incluso cuando la interceptación masiva se dirige a un individuo específico involucrado en un delito penal identificable. Por lo tanto, una orden de interceptación general, sin sospecha, es suficiente para desencadenar la interceptación masiva, ya sea para los propósitos de detección e investigación de delitos u otros" (párrafo 13).

"Dado que el artículo 8 se aplica a todas las etapas de la interceptación masiva, incluida la retención inicial de comunicaciones y datos de comunicaciones relacionados, el Tribunal ha establecido correctamente 'salvaguardas de principio a fin'. El problema es que el Tribunal no es claro en cuanto a la naturaleza legal de las 'salvaguardas de principio a fin'. Por un lado, ha utilizado un lenguaje imperativo ('debería hacerse', 'debería estar sujeto', 'debería autorizarse', 'debería ser informado', 'debe justificarse', y 'debería registrarse escrupulosamente', 'también debería estar sujeto', 'es imperativo que el remedio debería') y las ha llamado 'salvaguardas fundamentales' e incluso 'salvaguardas mínimas'. Pero, por otro lado, ha diluido estas salvaguardas en 'una evaluación global del funcionamiento del régimen', permitiendo un intercambio entre las salvaguardas. Parece que al final del día cada salvaguardia individual no es obligatoria, y el lenguaje prescriptivo del Tribunal no corresponde realmente a características no negociables del sistema doméstico. En algunos rincones de Europa, los servicios secretos celosos se sentirán fuertemente tentados a aprovechar la forma muy laxa del Tribunal de formular estándares legales y las personas inocentes pagarán el precio tarde o temprano" (párrafo 15).

Propuesta de un régimen más estricto para la interceptación masiva, incluyendo autorización judicial previa

"[E]l régimen mencionado anteriormente no constituye un conjunto suficiente de garantías de los derechos del artículo 8 y 10. [H]a llegado el momento de no prescindir de las garantías fundamentales de la autorización judicial, la supervisión y la revisión *ex post facto* en el campo de la interceptación masiva. Como cuestión de principio, la supervisión judicial de principio a fin de la interceptación masiva está justificada por la naturaleza extremadamente intrusiva de este proceso. No veo por qué un Estado regido por el estado de derecho no debería confiar en sus jueces en funciones, en última instancia en sus jueces más antiguos y experimentados, para decidir sobre tales asuntos. A menos que el Tribunal crea que los órganos cuasi judiciales son más independientes que los tribunales ordinarios... [...] la independencia de los órganos cuasi judiciales no es un hecho dado. Además, si los tribunales ordinarios son competentes para autorizar, supervisar y revisar la interceptación de comunicaciones en procedimientos penales altamente complejos, como investigaciones sobre crimen organizado y terrorismo, no entiendo por qué no deberían ser competentes para realizar exactamente la misma función con respecto a la operación de un proceso de interceptación masiva. Por lo tanto, ni la independencia ni la competencia de los tribunales ordinarios deberían ser cuestionadas con el propósito de construir una arquitectura de salvaguardias compatible con la Convención en un régimen de interceptación masiva. Un Estado que cree que su poder judicial en funciones no es apto para realizar estas funciones tiene un problema serio con el estado de derecho" (párrafo 19).

"[E]l control judicial debe abarcar la elección de los portadores específicos y los selectores fuertes. Por específico me refiero a los portadores individuales y selectores fuertes, no a ´tipos´ o ´categorías´ de portadores o selectores, lo que sería un cheque en blanco para que la autoridad interceptora elija lo que le guste" (párrafo 20).

"En el caso de un sistema de doble cerradura, por el cual el juez considera las órdenes previamente decididas por un político o un funcionario administrativo, la supervisión judicial no debe limitarse a la posibilidad de anular la decisión administrativa cuando el juez considere que el político o el funcionario administrativo actuó de manera irrazonable. Esto no sería una verdadera autorización judicial ya que las pruebas de necesidad y proporcionalidad requeridas por la Convención son más exigentes que la mera prueba de razonabilidad" (párrafo 21).

"Como mencioné en *Szábo y Vissy*, la Convención no permite la ´pesca de datos´, o expediciones ´exploratorias´, ni en forma de vigilancia no dirigida basada en selectores no específicos, ni en forma de vigilancia basada en selectores fuertes dirigidos a comunicaciones sobre el sujeto interceptado objetivo[...]" (párrafo 22).

"[C]ualquier objetivo de vigilancia siempre debe ser identificado o identificable de antemano basado en una sospecha razonable. Para no dejar dudas, la interceptación masiva solo debería ser admisible sobre la base de selectores fuertes dirigidos a las comunicaciones desde y hacia el sujeto interceptado objetivo cuando existe una sospecha razonable de que está involucrado en las categorías legalmente definidas de delitos graves o actividades que son perjudiciales para la seguridad nacional sin ser necesariamente criminales" (párrafo 23).

"La autorización judicial debería extenderse a la autorización de vigilancia de comunicaciones o datos de comunicaciones relacionados, incluidos datos privilegiados y confidenciales, con la única excepción de casos urgentes, cuando el juez competente no está disponible inmediatamente, donde la autorización puede ser dada por un fiscal público, sujeto al posterior respaldo del juez competente" (párrafo 24).

"La ley nacional debería proporcionar un régimen específico de protección para las comunicaciones profesionales privilegiadas de parlamentarios, médicos, abogados y periodistas. Dado que la recolección masiva indiscriminada y sin sospecha de comunicaciones frustraría la protección de la información legalmente protegida y confidencial, esto solo puede garantizarse efectivamente mediante la autorización judicial de la interceptación de dichas comunicaciones

cuando se presentan pruebas que respaldan una sospecha razonable de delitos graves o conductas perjudiciales para la seguridad nacional cometidas por estos profesionales. Además, cualquier comunicación de estas categorías de profesionales cubierta por su secreto profesional, si se intercepta por error, debe ser destruida inmediatamente. La ley nacional también debería prever la prohibición absoluta de cualquier interceptación de comunicaciones cubiertas por el secreto religioso" (párrafo 25).

"La supervisión judicial no debería detenerse al inicio de la operación de la interceptación. Si la operación real del sistema de interceptación estuviera oculta a la supervisión del juez, la intervención inicial de un juez podría ser fácilmente socavada y privada de cualquier efecto real, convirtiéndola en una salvaguardia meramente virtual y engañosa. Por el contrario, el juez debería acompañar todo el proceso, con un examen regular y vigilante de la necesidad y proporcionalidad de la orden de interceptación, en vista de los datos interceptados obtenidos. A menos que reciba retroalimentación constante de la autoridad interceptora, el juez autorizante no sabrá cómo se está utilizando realmente la autorización. En caso de incumplimiento de la orden de interceptación, el juez debería poder ordenar su cese inmediato y la destrucción de los datos obtenidos ilegalmente. Lo mismo debería aplicar en caso de falta de necesidad de proceder con la operación, por ejemplo, porque los datos obtenidos no son de interés para los fines perseguidos por la orden de interceptación. Solo un juez investido con el poder de tomar tales decisiones vinculantes puede proporcionar una garantía efectiva de la legalidad del material que se conserva. En resumen, el juez debería estar facultado para llevar a cabo una revisión regular de la operación del sistema, incluidos todos los registros de interceptación y documentos clasificados que lo acompañan, con el fin de evitar interferencias innecesarias y desproporcionadas con los derechos en virtud de los artículos 8 y 10" (párrafo 26).

"[L]a revisión *ex post facto* del uso hecho de una orden de interceptación también debería desencadenarse mediante la notificación a la persona objetivo. Cuando nada impide la notificación de la persona cuyas comunicaciones han sido interceptadas, esto le permitiría impugnar en un procedimiento judicial justo y contradictorio los motivos de dicha interceptación. Es, por lo tanto, altamente especulativo, por decir lo menos, pretender que un sistema que no depende de la notificación del sujeto interceptado ´puede incluso ofrecer mejores garantías de un procedimiento adecuado que un sistema basado en la notificación´. Nadie se preocupa más por los intereses del sujeto interceptado que el propio sujeto" (párrafo 27).

"[...] En este caso, es imperativo imponer al juez competente la carga de evaluar, por su propia iniciativa (*ex proprio motu*) o por iniciativa de un tercero (por ejemplo, un fiscal público), la forma en que se ejecutó la orden de interceptación con el fin de determinar si los datos en cuestión fueron recopilados legalmente y deben conservarse o destruirse; el sujeto interceptado debe entonces ser representado por un abogado [...]" (párrafo 28).

"Por último, pero no menos importante, los recursos humanos y financieros de supervisión y las capacidades deberían coincidir con la escala de las operaciones que se supervisan, de lo contrario todo el sistema será una mera fachada que cubre el proceso administrativo discrecional de las autoridades interceptoras" (párrafo 29).

2.6. TRIBUNAL EUROPEO DE DERECHOS HUMANOS (TEDH), "ZOLTÁN VARGA V. ESLOVAQUIA". CASO N° 58361/12. 20/7/2021.

HECHOS

El Servicio de Inteligencia Eslovaco (SIS) sospechaba que un expolicía, quien colaboraba con un grupo financiero, estaba implicado en actividades delictivas. En consecuencia, el SIS solicitó al Tribunal Regional de Bratislava tres órdenes de vigilancia. La primera orden autorizó la vigilancia en su departamento. La segunda orden amplió esta vigilancia a una tercera persona no identificada. La tercera permitió al SIS controlar al expolicía mediante grabaciones de audio y vídeo. En 2011, el expolicía, a través de un documento anónimo, descubrió que había sido investigado. Al investigar más a fondo, encontró que el Tribunal Regional había intervenido y de que una Comisión Parlamentario estaba investigando el uso de técnicas de inteligencia utilizado por el SIS. En junio de 2011, la persona presentó una queja ante el Tribunal Constitucional de Eslovenia, argumentando que las órdenes del Tribunal Regional y la vigilancia ejercida por el SIS le habían generado un perjuicio. En tal sentido, solicitó la destrucción de la información recopilada y una compensación económica. En marzo de 2012, el Tribunal Constitucional aceptó la queja contra las órdenes del Tribunal Regional, pero no otorgó la reparación en concepto de daños. Al respecto, el Tribunal Constitucional determinó que el Tribunal Regional violó los derechos del expolicía al no especificar el plazo para informar sobre la vigilancia. Además, afirmó que no tenía jurisdicción sobre el SIS y no podía ordenar la destrucción de la información obtenida durante la vigilancia.

DECISIÓN

El Tribunal Europeo de Derechos Humanos, por unanimidad, consideró que Eslovaquia era responsable por la violación del artículo 8 del Convenio Europeo de Derechos Humanos al respeto de su vida privada.

ARGUMENTOS

1. Vigilancia electrónica. Derecho a la privacidad. Control judicial. Control de constitucionalidad. Orden judicial.

"Aunque esta cuestión no ha sido objeto de controversia entre las partes, el Tribunal considera oportuno reiterar que, en virtud de su jurisprudencia, las medidas de vigilancia secreta y de almacenamiento, tratamiento y utilización de datos personales entran en principio en el ámbito de aplicación de la noción de vida privada a efectos del artículo 8 del Convenio (véanse, por ejemplo, *Hambardzumyan v. Armenia* y *Leander v. Suecia*)" (párrafo 144).

"Si bien tampoco se ha cuestionado la existencia de una interferencia con los derechos del demandante reconocidos en el artículo 8, el Tribunal observa que el presente caso presenta ciertas peculiaridades, en relación con el estado de las instalaciones en las que se implementaron las órdenes 1 y 2, el hecho que su ejecución podría haber afectado, al menos en parte, únicamente a terceros, y la incertidumbre sobre lo que estaba ocurriendo en dichos locales y lo que realmente fue controlado, grabado y posteriormente utilizado por el SIS o cualquier otra autoridad" (párrafo 145).

"El Tribunal observa que no se le han presentado productos de la implementación de las tres órdenes para su evaluación, en particular en cuanto a si el seguimiento y la recopilación, el almacenamiento y el uso de datos realmente se referían a la ´vida privada´ del demandante" (párrafo 146).

“Es cierto que el Tribunal Constitucional consideró una violación de los derechos del demandante en virtud del artículo 8 del Convenio, en relación con la emisión de las tres órdenes por el Tribunal Regional, y que, esencialmente sobre la base de esa conclusión y por extensión, el Tribunal Regional consideró en un procedimiento diferente que el SIS había violado el derecho del demandante a la protección de su integridad personal mediante la ejecución de estas órdenes y la producción de diversos materiales procedentes de su ejecución. Si bien estas conclusiones presuponen esencialmente la existencia de una injerencia en el derecho del solicitante a la protección de su ´vida privada´, ninguna de ellas ha sido respaldada ni acompañada de ningún análisis o detalle al respecto” (párrafo 147).

“No se discute que el demandante fue sometido a vigilancia sobre la base de las tres órdenes y que el SIS y el Tribunal Regional conservan diversos materiales procedentes de la ejecución de dichas órdenes y que le conciernen. En vista de las conclusiones de dichos tribunales internos y de la naturaleza específica de las medidas de vigilancia encubierta, que inherentemente hace difícil, sino imposible, que la persona interesada establezca los hechos en detalle, el Tribunal está dispuesto a aceptar que la implementación de las tres órdenes y el material resultante de ellas, al menos en parte, se referían a la ´vida privada´ del solicitante” (párrafo 148).

“La implementación de las tres órdenes y la producción y retención de los diversos materiales resultantes de ellas constituyó en consecuencia una interferencia con el derecho del demandante al respeto de su vida privada” (párrafo 149).

2. Vigilancia electrónica. Orden judicial. Arbitrariedad. Razonabilidad. Principio de proporcionalidad. Control de constitucionalidad. Democracia.

“Para determinar si la injerencia implicó una violación del artículo 8 de la Convención, el Tribunal debe examinar si fue ´conforme a la ley´, persiguió uno o más fines legítimos tal como se definen en el segundo párrafo de ese artículo y fue ´necesario en una sociedad democrática´ para lograr tal objetivo u objetivos (ver, por ejemplo, *Kvasnica v. Eslovaquia*, 9 de junio de 2009)” (párrafo 150).

“En cuanto al criterio ´conforme a derecho´, el Tribunal reitera su reiterada jurisprudencia según la cual este criterio no sólo exige que la medida impugnada tenga algún fundamento en el derecho interno, sino que también se refiere a la calidad del derecho en cuestión, lo que significa que debe ser accesible al interesado y previsible en cuanto a sus efectos. La ley debe ser compatible con el estado de Derecho, lo que significa que debe proporcionar una medida de protección legal contra la injerencia arbitraria de las autoridades en los derechos salvaguardados por el párrafo 1 del artículo 8. Especialmente cuando un poder del ejecutivo se ejerce en secreto, los riesgos de arbitrariedad son evidentes. Dado que la aplicación en la práctica de medidas de vigilancia secreta no está abierta al escrutinio de los individuos interesados ni del público en general, sería contrario al Estado de Derecho que la discrecionalidad legal concedida al ejecutivo se expresara en términos de un control sin restricciones fuerza. En consecuencia, la ley debe indicar el alcance de dicha discrecionalidad conferida a las autoridades competentes y la forma de su ejercicio con suficiente claridad, teniendo en cuenta el objetivo legítimo de la medida en cuestión, para brindar al individuo una protección adecuada contra injerencias arbitrarias (ver, por ejemplo, *Segerstedt-Wiberg y otros v. Suecia*)” (párrafo 151).

3. Ley. Control de constitucionalidad. Vigilancia electrónica. Orden judicial.

“La Corte observa que la ejecución de las órdenes condujo directamente a la producción del material primario. Por consiguiente, estaban intrínsecamente conectados y serán examinados juntos” (párrafo 152).

“Es indiscutible que la ejecución de las tres órdenes tenía en principio una base legal, a saber, las disposiciones respectivas de la Ley del PP [Ley de Protección de la Privacidad], y que, como lo exigían esas disposiciones, las órdenes fueron emitidas por un juez. No se ha hecho ningún reproche en cuanto a la claridad o accesibilidad de dichas normas” (párrafo 153).

“Sin embargo, como estableció posteriormente el Tribunal Constitucional, las órdenes tenían defectos fundamentales que las hacían ilegales e inconstitucionales. Si bien estas deficiencias eran imputables al tribunal de emisión, fue esencialmente sobre la base de la anulación de las órdenes por el Tribunal Constitucional que el Tribunal Regional consideró, resolviendo el recurso del demandante en su acción de protección de la integridad personal, que la ejecución de las órdenes del SIS también había violado sus derechos” (párrafo 154).

“El Tribunal observa que la sentencia del Tribunal Regional no implicaba ninguna evaluación de los actos del SIS como tales y que dicha evaluación no había sido realizada por el Tribunal Constitucional” (párrafo 155).

“[E]l Tribunal observa que en el procedimiento ante el Tribunal Constitucional el demandante presentó un documento procedente del Tribunal Regional según el cual, en el momento pertinente, esa judicatura no había tenido a su disposición el equipo técnico requerido por Ley para el procesamiento de información clasificada. En consecuencia, las órdenes como en el presente caso fueron presentadas por el organismo que las solicitó. El Tribunal señala que en el mismo procedimiento constitucional el Tribunal Regional añadió que era práctica común en aquel momento que el SIS no especificara en detalle los motivos individuales detrás de una solicitud de medios técnicos de recopilación de información (TMGI). Estas presentaciones tienden a retratar la imagen de una agencia de inteligencia que redacta por sí misma las órdenes que autorizan su interferencia con los derechos humanos y las libertades fundamentales individuales y la de un tribunal que respalda esos borradores sin verificar genuinamente los hechos” (párrafo 156).

“En estas circunstancias, el Tribunal considera que las deficiencias de las tres órdenes establecidas por el Tribunal Regional contaminaron inherentemente el uso del TMGI por parte del SIS contra el solicitante sobre esa base” (párrafo 157).

“En lo que respecta a cualquier otro medio de protección jurídica contra las injerencias arbitrarias, el Tribunal señala que el artículo 4, apartado 6, de la Ley PP establece el deber del juez emisor de examinar sistemáticamente si los motivos por los que se autorizó el uso del TMGI siguen existiendo. Sin embargo, en el presente asunto, no hay indicios de que los jueces que dictaron los mandamientos judiciales en cuestión llevaran a cabo ninguna tarea de control sobre la base de dicha disposición. En la medida en que el Tribunal conoce el contenido de sus expedientes, éstos sugieren más bien una pauta de inacción, que se ve respaldada de nuevo por la alegación del Tribunal Regional en el procedimiento constitucional relativo a la orden 3. En particular, declaró que, como era habitual en aquella época, el SIS no había presentado al Tribunal Regional ningún registro sobre la ejecución de dicha orden ni el acta de destrucción de los registros así obtenidos. Además, el Tribunal Regional añadió que, en aquella época, estas cuestiones no se regían por ninguna norma específica (párrafo 158)”.

“En cuanto a cualquier revisión posterior de la ejecución de las órdenes impugnadas, la actitud pasiva del Tribunal Regional culminó con la destrucción de sus expedientes relativos a la ejecución de las tres órdenes. Otras autoridades, como el PPS [Oficina de Enjuiciamientos Especiales del Ministerio Público] y la Oficina de Gobierno, han negado directamente tener competencia alguna respecto de la legalidad de las actuaciones del SIS. Aunque la situación del demandante fue remitida al Comité Parlamentario Especial, el material presentado al Tribunal no contiene nada que demuestre que el Comité pudiera examinar, o haya examinado, algún aspecto individual de

la misma. A este respecto, el Tribunal toma nota también de las conclusiones del Tribunal Regional, en un recurso de acceso al reglamento interno del SIS relativo a la conservación de sus registros, según las cuales el control de dicho organismo era principalmente político y que en el caso del asociado del demandante el Comité no tenía poder para decidir sobre ninguna reclamación individual contra el SIS para la protección de la integridad personal o compensación por conducta oficial errónea del SIS. En la medida en que debería haberse reforzado el control parlamentario mediante la creación de una comisión especial para la supervisión del uso del TMGI, el Tribunal observa que, si bien la respectiva modificación de la Ley del PP está en vigor desde hace tiempo, no hay indicios de que la comisión haya sido realmente creada y haya asumido sus funciones. Además, según lo establecido por los tribunales y reconocido en parte por el Gobierno, la ejecución de las órdenes quedaba fuera del ámbito del poder judicial administrativo y del ámbito de aplicación de la Ley SL [Ley de Responsabilidad del Estado]" (párrafo 159).

"Es cierto que el Tribunal Regional, actuando como tribunal de apelación en el recurso del demandante para la protección de la integridad personal, consideró finalmente que la ejecución de las tres órdenes había violado sus derechos. Sin embargo, [...] esto parece haberse basado en el mero hecho de que las órdenes fueron anuladas, sin que el Tribunal Constitucional o el Tribunal Regional hicieran ninguna revisión sustantiva de las acciones del SIS (véase, *mutatis mutandis, Akhlyustin v. Rusia*)" (párrafo 160).

"El Tribunal también señala que la sentencia del Tribunal Regional parece ser un giro de los acontecimientos después de casi una década en la que el demandante buscó activamente, aunque en vano, un foro en el que examinar sus reclamaciones. Ese esfuerzo estuvo marcado por una referencia legislativa inviable de la Ley del PP a la Ley SL, remisiones jurisdiccionales circulares del Tribunal Constitucional al Tribunal Regional, junto con remisiones inútiles entre otras autoridades y de éstas a los tribunales administrativos" (párrafo 161).

"En resumen, en vista de la falta de claridad de las normas jurisdiccionales aplicables, la falta de procedimientos para la implementación de las normas existentes y las fallas en su aplicación, al implementar las tres órdenes, el SIS prácticamente gozó de una discrecionalidad equivalente a un poder ilimitado, no ir acompañado de una medida de protección contra la interferencia arbitraria como exige el estado de derecho. En consecuencia, no fue ´conforme a la ley´ a los efectos del artículo 8.2 del Convenio" (párrafo 162).

"A este respecto, el Tribunal señala que la cuestión de la eficiencia del control judicial en el contexto de la autorización de TMGI parece ser una preocupación duradera independientemente de la promulgación y entrada en vigor de la Ley PP en 2003" (párrafo 163).

"En lo que respecta al material primario resultante de la implementación de la orden 3, [...] esta orden fue anulada por el Tribunal Constitucional por ser ilegal e inconstitucional y el Tribunal Regional consideró que su implementación había violado el derecho del demandante a protección de su integridad personal. En consecuencia, parecería fuera de toda controversia, y de hecho así lo sostiene el propio Gobierno, que el material primario en cuestión cae bajo el régimen del artículo 7(3) de la Ley PP, que exige su destrucción en presencia de un juez" (párrafo 164).

"[S]egún lo establecido por el Tribunal Constitucional, dicho material no fue destruido sino almacenado por el SIS en su sistema de información en virtud del artículo 17(6) de la Ley del SIS. Aunque el Tribunal Constitucional consideró específicamente que era competencia del Tribunal Regional garantizar el cumplimiento por parte del SIS de la disposición citada de la Ley del PP, este último había negado repetidamente tener competencia para hacerlo" (párrafo 165).

“A este respecto, el Tribunal también observa las conclusiones del Tribunal Regional, en el contexto de la acción de protección de la integridad personal del demandante, con respecto a su solicitud de que se ordene la destrucción del material impugnado, de que le era imposible , al tribunal o a un agente judicial identificar con precisión el material en cuestión, lo que en la práctica también significaba que no se podía presentar tal reclamación ante los tribunales ordinarios” (párrafo 166).

“En cuanto al almacenamiento tanto del material primario de la ejecución de la orden 3 como del material derivado de la ejecución de las tres órdenes en virtud del artículo 17(6) de la Ley SIS, el Tribunal señala que aspectos importantes del régimen jurídico aplicable se rigen por un reglamento interno del director del SIS dictado en virtud del artículo 17(8) de la Ley SIS. En virtud de dicha disposición, este reglamento debe regular cuestiones tales como las normas relativas a la autoridad para acceder a dicho material, la divulgación de los datos procedentes del mismo y el alcance y el momento de su destrucción. Sin embargo, su contenido real no puede ser evaluado, ya que el reglamento es clasificado y no ha sido revelado ni al Tribunal ni a la demandante” (párrafo 167).

“No parece haber ningún organismo con autoridad para revisar las acciones tomadas por el SIS en la implementación de órdenes para el uso de TMGI y, por extensión, para supervisar su cumplimiento con su propia regulación interna” (párrafo 168).

“[E]l almacenamiento tanto del material primario de la implementación de la orden 3 como del material derivado de la implementación de las tres órdenes bajo la sección 17(6) de la Ley SIS estaba sujeto a reglas confidenciales que fueron adoptadas y aplicado por el SIS, sin ningún elemento de control externo. Estas normas carecían claramente de accesibilidad y no proporcionaban al solicitante ninguna protección contra injerencias arbitrarias en su derecho al respeto de su vida privada” (párrafo 169).

“[S]alvo que el Gobierno haya argumentado lo contrario, el Tribunal considera que, desde la anulación de la orden 3 por el Tribunal Constitucional, la retención por el SIS del material primario procedente de su ejecución ha sido como tal carece de fundamento jurídico suficiente” (párrafo 170).

2.7. TRIBUNAL EUROPEO DE DERECHOS HUMANOS, "EKIMDZHIEV Y OTROS V. BULGARIA". CASO N° 70078/12. 11/1/2022.

HECHOS

En 1997, Bulgaria promulgó la Ley de Medios Especiales de Vigilancia, que regulaba el uso de vigilancia secreta en el país. En junio de 2007, el Tribunal Europeo de Derechos Humanos (TEDH) dictó sentencia en el caso *Association for European Integration and Human Rights* y *Ekimdzhiev v. Bulgaria*, y consideró vulnerados los artículos 8 y 13 del Convenio Europeo de Derechos Humanos. En diciembre de 2008, en respuesta a esta sentencia, el Parlamento búlgaro realizó modificaciones a la Ley promulgada en 1997. Estas enmiendas permitieron la creación de la Oficina Nacional para el Control de Medios Especiales de Vigilancia, autoridad independiente cuyos cinco miembros serían elegidos por el Parlamento. En octubre de 2009, antes de que la Oficina Nacional pudiera comenzar a operar, el Parlamento aprobó nuevas enmiendas que abolieron la Oficina y la reemplazaron por un subcomité parlamentario especial. En agosto de 2013, otra enmienda a la Ley de 1997 restableció la Oficina Nacional como una "autoridad estatal independiente". Sus cinco miembros fueron elegidos por el Parlamento en diciembre de 2013, y la Oficina comenzó su trabajo a principios de 2014. En 2015, el Tribunal Constitucional de Bulgaria declaró inconstitucionales varios artículos de la Ley de Comunicaciones Electrónicas de 2007 relacionadas con la retención de datos. En respuesta, el Parlamento añadió nuevos artículos a la Ley de Comunicaciones Electrónicas y un nuevo artículo al Código de Procedimiento Penal, estableciendo un nuevo marco para la retención y acceso a datos de comunicaciones.

En octubre de 2012, los demandantes (dos abogados y dos organizaciones no gubernamentales) presentaron una demanda ante el Tribunal Europeo de Derechos Humanos. Los demandantes argumentaron que el sistema de vigilancia secreta y de retención de datos de comunicaciones en Bulgaria violaba su derecho al respeto de la vida privada y la correspondencia bajo el artículo 8 del Convenio, y que no disponían de un recurso efectivo al respecto, en violación del artículo 13. Por su parte, el Gobierno búlgaro argumentó que los demandantes no podían reclamar ser víctimas de una violación de sus derechos, ya que no habían demostrado que sus comunicaciones hubieran sido interceptadas o sus datos accedidos. Además, sostuvo que existían recursos efectivos disponibles en la legislación búlgara que los demandantes no habían agotado.

DECISIÓN

El Tribunal Europeo de Derechos Humanos consideró que Bulgaria era responsable por la vigilancia secreta, retención y posterior acceso a los datos de las comunicaciones personales (artículo 8 del Convenio Europeo de Derechos Humanos).

ARGUMENTOS

1. Derecho a la privacidad. Derecho a la vida privada y familiar. Protección de datos personales. Derecho a la intimidad. Vigilancia electrónica.

“Cuando en 2007 revisó el procedimiento de autorización en virtud de la Ley de 1997, el Tribunal concluyó que, si se respetaba estrictamente, dicho procedimiento proporcionaba salvaguardias sustanciales contra la vigilancia arbitraria o indiscriminada (véase *Asociación para la Integración Europea y los Derechos Humanos* y *Ekimdzhiev*). La sofisticación de las disposiciones pertinentes ha aumentado desde entonces. Estos procedimientos, sin embargo, deben examinarse no sólo tal y como existen sobre el papel, sino también tal y como funcionan en la práctica, en la medida en que ello pueda comprobarse sobre la base de fuentes oficiales fiables (compárese con caso *Roman Zakharov*)” (párrafo 307).

“Los dos tribunales de Bulgaria que han emitido el mayor número de órdenes de vigilancia durante la última década fueron, por un amplio margen, el Tribunal de la ciudad de Sofía (hasta

2015) y el Tribunal Penal Especializado (desde 2015). Según un informe oficial publicado a principios de 2017, hasta abril de 2015 todos los jueces del Tribunal de la ciudad de Sofía que emitían órdenes de vigilancia no motivaban en absoluto sus decisiones, y en abril-agosto de 2015 solo motivaban, con pocas excepciones, de forma ´general y generalizada´. Así lo confirman las dos órdenes de vigilancia de 2012 y 2013 emitidas por dicho órgano jurisdiccional presentadas por los demandantes. Es cierto que, tras el escándalo que estalló en 2015 en relación con la forma en que el Tribunal la ciudad de Sofía tramitaba las solicitudes de vigilancia (y que posteriormente dio lugar a la destitución y condena penal de su presidente), los jueces competentes de dicho tribunal comenzaron a motivar sistemáticamente sus decisiones de emitir órdenes de vigilancia. Sin embargo, más o menos al mismo tiempo, el número de solicitudes de vigilancia dirigidas a ese tribunal disminuyó bruscamente, y el mayor número de esas solicitudes comenzó a presentarse ante el Tribunal Penal Especializado. De hecho, desde 2018, el Tribunal Penal Especializado ha estado emitiendo aproximadamente la mitad de todas las órdenes de vigilancia en Bulgaria" (párrafo 311).

"Como se desprende de dos sentencias recientes del Tribunal Penal Especializado, una treintena de órdenes de vigilancia emitidas por su presidente y vicepresidentes tenían un contenido totalmente general, estaban redactadas en términos lo suficientemente generales como para poder referirse a cualquier posible solicitud de vigilancia, y carecían de cualquier referencia al caso concreto al que se referían, salvo el número de la solicitud. No hay ninguna razón para pensar que esas órdenes fueran de algún modo excepcionales y representaran algo distinto de la práctica normal en ese tribunal" (párrafo 312).

"[S]e puede concluir que no se han motivado debidamente las decisiones de emitir la gran mayoría de todas las órdenes de vigilancia emitidas en Bulgaria en la última década. Esto es de particular relevancia, ya que la provisión contemporánea de razones es una salvaguardia vital contra la vigilancia abusiva (véase *Dragojević v. Croacia*; *Dudchenko v. Rusia*; y *Liblik y otros v. Estonia*). Esto se debe a que la motivación, aunque sea sucinta, es la única manera de garantizar que el juez que examina una solicitud de vigilancia ha revisado adecuadamente la solicitud y los materiales que la respaldan, y ha dirigido realmente su mente a las cuestiones de si la vigilancia sería una injerencia justificada y proporcionada en los derechos del artículo 8 de la persona o personas contra las que se dirigirá, y de cualquier persona o personas que puedan verse colateralmente afectadas por ella. En Bulgaria, esto es especialmente importante a la vista de lo dicho por los demandantes —que parece corroborada, entre otras cosas, por algunos acontecimientos recientes— de que los procedimientos penales pueden incoarse de forma frívola y abusiva, principalmente con el fin de permitir que se someta a alguien a vigilancia por motivos ocultos. Como demuestran las disposiciones adoptadas en el Tribunal de la ciudad de Sofía desde agosto de 2015, la motivación, independientemente de si se admite o se rechaza una solicitud de vigilancia, no es inalcanzable en la práctica, a pesar de los plazos bastante cortos para pronunciarse sobre dichas solicitudes" (párrafo 313).

"El primero de estos factores es la enorme carga de trabajo que suponen estas solicitudes, que por ley sólo pueden ser tramitadas por los presidentes o vicepresidentes de los respectivos tribunales. La Oficina Nacional ha llamado la atención en repetidas ocasiones sobre la insuficiencia de personal y medios puestos a disposición de la Sala Penal Especializada para tramitar adecuadamente todas las solicitudes de vigilancia presentadas a su presidente y vicepresidentes. El propio Tribunal Penal Especializado también ha llamado la atención sobre la carga de trabajo cada vez mayor que supone el gran volumen de solicitudes de vigilancia que se le presentan, y el Comité de ministros ya ha destacado la cuestión en el contexto de su supervisión de los casos *Asociación para la Integración Europea y los Derechos Humanos* y *Ekimdzhiev*" (párrafo 315).

"El segundo factor es el elevado porcentaje de solicitudes de vigilancia que se están admitiendo" (párrafo 316).

“El tercer factor es la posición expresa del Tribunal Penal Especializado de Apelación —que tiene competencia directa de supervisión sobre el Tribunal Penal Especializado— de que un juez que se ocupa de una solicitud de vigilancia sólo tiene que comprobar si se cumplen los requisitos formales para permitirla, sin entrar en los materiales en apoyo de la solicitud” (párrafo 317).

“[E]l Tribunal no puede estar convencido de que los procedimientos de autorización de la vigilancia secreta, tal como funcionan en la práctica en Bulgaria, garanticen efectivamente que dicha vigilancia sólo se autorice cuando sea realmente necesaria y proporcionada en cada caso” (párrafo 321).

“El control adicional efectuado por las autoridades de vigilancia tras la concesión de la autorización judicial no puede remediar esta falta de control judicial adecuado, por dos razones. En primer lugar, dicho control se limita a la incompatibilidad *ratione materiae* o a errores manifiestos. En segundo lugar, los casos en los que se ha recurrido a esta garantía adicional son, al parecer, extremadamente raros” (párrafo 322).

“En Bulgaria, tres autoridades pueden supervisar la utilización de medios especiales de vigilancia: a) el juez que ha emitido la orden de vigilancia respectiva; b) la Oficina Nacional; y c) una comisión parlamentaria especial” (párrafo 335).

“La sofisticación de este sistema va mucho más allá de los dispositivos condenados por el Tribunal en la sentencia *Asociación para la integración europea y los derechos humanos* y *Ekimdzhiev*. No obstante, no alcanza el nivel de eficacia exigido en varios aspectos” (párrafo 336).

“[E]l principal órgano de supervisión, la Oficina Nacional, adolece de varias deficiencias que socavan su eficacia en la práctica” (párrafo 338)

“En primer lugar, no existe ninguna garantía de que todos sus miembros sean suficientemente independientes con respecto a las autoridades que deben supervisar. Por ley, las personas con experiencia profesional en las fuerzas del orden o en los servicios de seguridad pueden ser miembros de la Oficina Nacional. Una vez cumplido su mandato de cinco años (que, se concede, puede renovarse), tienen derecho a recuperar sus puestos anteriores. Este mecanismo potencial de ´puerta giratoria´ puede suscitar recelos sobre la independencia práctica de dichos miembros de la Oficina y sobre posibles conflictos de intereses por su parte (véase, *mutatis mutandis*, *Centrum för rättvisa*). De hecho, el actual presidente de la Oficina procedía directamente de la Agencia Estatal de Seguridad Nacional, y el vicepresidente que fue elegido en 2018 y dimitió a mediados de 2021 (tras haber sido sancionado por las autoridades de los Estados Unidos de América por graves acusaciones de corrupción) había estado empleado por los servicios de seguridad durante más de dos décadas y media antes de incorporarse a la Oficina” (párrafo 339).

“Otro aspecto de la organización de la Oficina Nacional suscita nuevas dudas a este respecto. Antes de ser nombrados para sus puestos, sus miembros deben someterse a un control de seguridad por parte de una de las mismas autoridades cuya labor supervisa la Oficina: la Agencia Estatal de Seguridad Nacional. Esto crea un evidente conflicto de intereses para dicha Agencia. Si posteriormente revoca la habilitación de seguridad de los miembros de la Oficina, estos deben ser cesados de su puesto, ya que automáticamente dejan de ser elegibles para ocuparlo; eso ya ocurrió una vez en 2017-18. Aunque la decisión de la Agencia de revocar una habilitación de seguridad es susceptible de control jurisdiccional, esa posibilidad de que influya en los miembros de la Oficina puede afectar a la independencia de esta y a la objetividad y rigor de su labor de supervisión, especialmente en lo que respecta a dicha Agencia” (párrafo 340).

“En tercer lugar, no parece que, al realizar inspecciones *in situ*, los miembros de la Oficina Nacional y sus empleados puedan acceder sin restricciones a todos los materiales pertinentes que obren en poder de las autoridades fiscales y de la Agencia Estatal de Seguridad Nacional, especialmente los materiales que les permitan comprobar el fundamento de las solicitudes de vigilancia

(sospecha razonable y proporcionalidad en cada caso). La Oficina también se ha quejado del suministro reiterado de información incorrecta por parte de la principal autoridad de vigilancia de Bulgaria, la Agencia de Operaciones Técnicas. Tal obstrucción debilita gravemente las capacidades de supervisión de la Oficina, y no puede considerarse justificada (compárese, *mutatis mutandis*, con *Roman Zakharov*). Facilitar a los miembros de la Oficina el acceso a todos los materiales del expediente de un caso penal no puede perjudicar a las investigaciones en curso, ya que dichos miembros tienen la más alta habilitación de seguridad y están sujetos al secreto profesional. El Comité de ministros ya ha llamado la atención también sobre esta cuestión" (párrafo 343)

"[L]a Oficina Nacional no está facultada para ordenar medidas correctivas, como la destrucción del material de vigilancia. Sólo puede poner las irregularidades en conocimiento de los jefes de las autoridades competentes y de la fiscalía, o del Consejo Superior de la Magistratura, para las irregularidades imputables a los jueces. La facultad de la Oficina de dar instrucciones parece referirse únicamente a instrucciones destinadas a mejorar las prácticas y no a instrucciones en casos concretos, como lo atestigua en particular su número limitado por año" (párrafo 344).

"[E]l sistema de supervisión de la vigilancia secreta en Bulgaria, tal como está organizado actualmente, no parece capaz de ofrecer garantías efectivas contra la vigilancia abusiva" (párrafo 347).

2. Protección de datos personales. Sistema informático. Vigilancia electrónica. Control judicial. Principio de legalidad. Medidas de seguridad.

"La legislación búlgara establece salvaguardias destinadas a garantizar que las autoridades sólo accedan a los datos de comunicaciones conservados cuando esté justificado. En primer lugar, sólo un número limitado de autoridades puede solicitar el acceso a esos datos, en el ámbito de sus respectivas competencias. Y lo que es más importante, dicho acceso sólo puede ser concedido por el presidente del tribunal competente o por un juez en quien se haya delegado esa facultad (para el acceso solicitado fuera del marco de un procedimiento penal ya pendiente), o por un juez del tribunal de primera instancia competente (para el acceso solicitado por un fiscal en el curso de un procedimiento penal)" (párrafo 400).

"No obstante, estas garantías no alcanzan el nivel de eficacia exigido en varios aspectos" (párrafo 401).

"Las solicitudes de acceso presentadas fuera del marco de un procedimiento penal ya pendiente deben exponer no sólo los motivos por los que se solicita el acceso a dichos datos y la finalidad para la que se solicitan, sino también contener una relación completa de las circunstancias que demuestran que los datos son necesarios para una finalidad pertinente. Por el contrario, las solicitudes de acceso presentadas en el curso de un procedimiento penal, aunque se espera que contengan información sobre el presunto delito en relación con el cual se solicita el acceso, no están expresamente obligadas a explicar, en términos concretos, por qué se necesitan realmente los datos en cuestión; sólo tienen que contener una descripción de las circunstancias en que se basa la solicitud de acceso, lo que parece ser un requisito totalmente menos estricto. Por lo tanto, la ley no deja claro en todas las situaciones que el acceso en cada caso individual sólo puede solicitarse y concederse si la interferencia resultante con los derechos del artículo 8 de la persona o personas afectadas es realmente necesaria y proporcionada" (párrafo 402).

"Al igual que en el caso del procedimiento de autorización de vigilancia secreta, otra posible deficiencia en esta fase es que, aunque el procedimiento de acceso a los datos debe desarrollarse necesariamente sin notificación a las personas cuyos datos de comunicaciones se solicitan, la autoridad que solicita el acceso no tiene la obligación de revelar al juez de forma completa y franca todos los elementos pertinentes para fundamentar su solicitud de acceso, incluidos los elementos que puedan debilitar sus argumentos" (párrafo 403).

“La ley tampoco exige que se adjunte material justificativo a la solicitud de acceso, lo que en muchos casos puede impedir que el juez que tramita la solicitud compruebe adecuadamente si está bien fundada” (párrafo 404).

“La ley tampoco exige que los jueces que examinan dichas solicitudes expongan los motivos por los que han decidido que conceder el acceso a los datos de las comunicaciones en cuestión era realmente necesario. Como ya se ha señalado en relación con el procedimiento para autorizar la vigilancia secreta, la motivación, aunque sea sucinta, es la única forma de garantizar que el juez que examina una solicitud de acceso ha examinado adecuadamente la solicitud y los materiales que la apoyan, y ha dirigido verdaderamente su mente a las cuestiones de si el acceso a los datos de las comunicaciones en cuestión constituiría una injerencia justificada y proporcionada en los derechos del artículo 8 de la persona o personas a cuyos datos se está accediendo, y de cualquier persona o personas que puedan verse colateralmente afectadas por ello” (párrafo 405).

“[L]os procedimientos para autorizar a las autoridades a acceder a los datos de comunicaciones conservados no garantizan efectivamente que dicho acceso se conceda únicamente cuando sea realmente necesario y proporcionado en cada caso” (párrafo 406).

“En Bulgaria, tres autoridades pueden supervisar la conservación de los datos de las comunicaciones y su posterior acceso por las autoridades: a) la Comisión de Protección de Datos Personales; b) el juez que ha emitido la orden de acceso; y c) la misma comisión parlamentaria que supervisa la vigilancia secreta” (párrafo 410).

“En virtud de la Ley de 2007, la Comisión de Protección de Datos de Carácter Personal puede a) solicitar a los proveedores de servicios de comunicaciones que le faciliten cualquier información pertinente para su mandato en ese ámbito, b) comprobar cómo cumplen esos proveedores su obligación de comunicar a los usuarios las violaciones de datos personales, y c) comprobar las medidas técnicas y organizativas adoptadas por esos proveedores para almacenar los datos de comunicaciones conservados (véanse los apartados 201 y 202 supra). También puede dar instrucciones vinculantes a los proveedores de servicios de comunicaciones y sancionarlos (véanse los apartados 203 y 204). Pero su mandato en virtud de la Ley de 2007 parece limitarse a supervisar a los proveedores de servicios de comunicaciones (véase el apartado 198 supra); no tiene competencias expresas en virtud de dicha Ley con respecto a las autoridades que pueden acceder a los datos de comunicaciones conservados” (párrafo 411).

“[E]n virtud de las disposiciones de la Ley de 2002, modificada en 2019 para transponer la Directiva (UE) 2016/680, la misma Comisión —así como la Inspección adscrita al Consejo Superior de la Magistratura— están encargadas de supervisar la forma en que las autoridades tratan cualquier dato personal con fines policiales. Pero nada indica que ninguna de estas dos autoridades haya hecho uso hasta ahora de esas competencias en relación con los datos de las comunicaciones” (párrafo 412).

“[E]l juez que ha emitido la orden de visita no está en condiciones de garantizar una supervisión eficaz. Es cierto que debe ser informado de la destrucción de los datos de comunicaciones irrelevantes o inútiles a los que hayan tenido acceso las autoridades. Pero ese juez no está facultado para ordenar medidas correctoras. Además, no está facultado ni se espera de él que realice inspecciones *in situ*, y desempeña sus funciones de supervisión únicamente sobre la base del informe presentado por las autoridades. Aunque se trata de una salvaguardia valiosa, este mecanismo es insuficiente para garantizar que no se abusa de los poderes de acceso a los datos” (párrafo 413).

“El principal órgano de supervisión, la comisión parlamentaria especial, puede supervisar tanto a los proveedores de servicios de comunicaciones como a las autoridades pertinentes, y dispone de amplios poderes de recopilación de información e inspección. Sus informes anuales

demuestran que realiza regularmente inspecciones a través de los expertos que emplea. Pero varias deficiencias merman su eficacia. En primer lugar, sus miembros no tienen por qué ser personas con cualificación o experiencia jurídica. En segundo lugar, no está facultado para ordenar medidas correctoras en casos concretos, como la destrucción de los datos de las comunicaciones conservados o a los que se haya accedido; sólo puede dar instrucciones destinadas a mejorar los procedimientos pertinentes. Si detecta irregularidades, sólo puede poner el asunto en conocimiento de las autoridades judiciales, o informar a los responsables de las autoridades competentes que solicitan el acceso y a los proveedores de servicios de comunicaciones" (párrafo 414).

"A la vista de las deficiencias expuestas, el sistema de control de la conservación de los datos de las comunicaciones y de su posterior acceso por las autoridades en Bulgaria, tal como está organizado actualmente, no parece capaz de ofrecer garantías efectivas contra las prácticas abusivas a este respecto" (párrafo 415).

3. Acceso a la justicia. Derecho de defensa. Legitimación. Indemnización. Prueba. Prueba digital. Acción de amparo.

"En 2009, Bulgaria estableció un recurso específico en relación con la vigilancia secreta: una reclamación de daños y perjuicios en virtud del artículo 2(1)(7) de la Ley de 1988. Pero ese recurso, aunque eficaz en algunos casos, adolece de tres graves limitaciones expuestas en los apartados 266 a 273 supra: (a) hasta ahora no ha podido aplicarse en ausencia de notificación previa por parte de la Oficina Nacional de que alguien ha sido sometido a vigilancia, (b) no implica un examen de la necesidad de la vigilancia en cada caso, y (c) no está abierto a las personas jurídicas" (párrafo 352).

"[L]a única forma de reparación disponible en tales procedimientos es la indemnización por daños y perjuicios; los tribunales no están facultados para ordenar la destrucción del material de vigilancia (véase, por ejemplo, *Big Brother Watch y otros*). El Comité de ministros ya ha destacado este punto en el contexto de su supervisión de la ejecución del caso *Asociación para la Integración Europea y los Derechos Humanos* y *Ekimdzhiev*" (párrafo 353).

"[L]os recursos novedosos disponibles en virtud de la Ley de 2002, modificada en 2019 para transponer la Directiva (UE) 2016/680, no han demostrado hasta ahora su eficacia en relación con la vigilancia secreta y, además, no están a disposición de las personas jurídicas" (párrafo 354).

"[L]la legislación búlgara no ofrece un recurso efectivo a todas las personas que sospechen, sin pruebas concretas, que han sido sometidas injustificadamente a vigilancia secreta. También se deduce que la objeción del Gobierno de que no se han agotado los recursos internos, que se unió al fondo, debe ser rechazada (párrafo 355).

"Ni la Ley de 2007 ni el artículo 159a de la Ley de Enjuiciamiento Criminal prevén un recurso contra la retención o el acceso a datos de comunicaciones" (párrafo 379).

"Nada indica que los recursos previstos en el artículo 38, apartados 1 y 7, el artículo 39, apartados 1 y 2, y el artículo 82, apartado 1, de la Ley de 2002, tal como quedaron redactados tras la modificación de 2019 destinada a transponer la Directiva (UE) 2016/680, se hayan utilizado hasta ahora para ofrecer reparación con respecto a la retención de datos de comunicaciones por los proveedores de servicios de comunicaciones o con respecto a su acceso y utilización por las autoridades. A falta de resoluciones de los órganos jurisdiccionales búlgaros, no corresponde a este Tribunal determinar si dichos recursos, que son de aplicación general, pueden operar en tales casos o de qué modo. Es cierto que dichos recursos son novedosos y que forman parte de una rama del Derecho que se ha desarrollado hace relativamente poco tiempo. Pero correspondía al Gobierno explicar su modo de funcionamiento y, en la medida de lo posible, apoyar sus explicaciones con ejemplos concretos (véanse, *mutatis mutandis*, las sentencias *Roman Zakharov*

y *Mustafa Sezgin Tanrıkulu*). Sin embargo, el Gobierno se mostró vago al respecto, contentándose con decir que la enmienda de 2019 había introducido disposiciones que regulaban la responsabilidad de los proveedores de servicios de comunicaciones y de las autoridades pertinentes en relación con los datos de comunicaciones retenidos y a los que se haya accedido (contrasten las circunstancias en *Ringler v. Austria*). A falta de más detalles sobre el funcionamiento real de estos recursos con respecto a los datos de las comunicaciones, no puede aceptarse que actualmente sean efectivos a este respecto. Además, esos recursos no están abiertos a las personas jurídicas" (párrafo 380).

"Tampoco hay pruebas de que exista un recurso disponible en virtud del derecho general de responsabilidad civil" (párrafo 381).

4. Derecho a la información. Consentimiento informado. Protección de datos personales. Identificación de personas. Publicidad. Derecho de defensa.

"[L]a Oficina Nacional sólo debe notificar a alguien que ha sido sometido a vigilancia secreta si ello ha sucedido ilegalmente, mientras que, en virtud de la jurisprudencia del Tribunal, dicha notificación, a falta de un recurso disponible sin notificación previa, es necesaria en todos los casos, tan pronto como pueda realizarse sin poner en peligro la finalidad de la vigilancia (véase *Klass y otros v. Alemania*; *Weber y Saravia v. Alemania*; y, más recientemente, *Roman Zakharov*). Es revelador a este respecto que el número de notificaciones realizadas por la Oficina cada año en relación con el número anual de órdenes de vigilancia sea muy pequeño (compárense los cuadros de los apartados 55 y 135 supra). Además, la Oficina sólo está obligada a notificar a personas físicas, no a personas jurídicas (véase el apartado 130 supra), un punto ya señalado por el Comité de ministros en el contexto de su supervisión de la ejecución del caso *Asociación para la Integración Europea y los Derechos Humanos* y *Ekimdzhiev*" (párrafo 349).

"El Gobierno no alegó, y no hay indicios de ello, que hasta la fecha se hayan dado casos en los que se haya efectuado dicha notificación en virtud del artículo 54, apartado 4, de la Ley de 2002, modificada en 2019 para transponer la Directiva (UE) 2016/680 (véase el apartado 220 supra). Tampoco parece que haya habido hasta ahora casos en los que las personas hayan podido obtener información sobre la vigilancia secreta en virtud del artículo 55, apartado 3, in fine, del artículo 56, apartado 6, *in fine*, o del artículo 57, apartados 1 y 2, de la misma Ley, en su redacción posterior a la modificación de 2019" (párrafo 350).

"Al mismo tiempo [...] la notificación por parte de la Oficina Nacional suele ser un requisito previo para presentar una reclamación por daños y perjuicios en virtud del artículo 2, apartado 1, punto 7, de la Ley de 1988; la única otra situación en la que se puede presentar una reclamación de este tipo es cuando la vigilancia secreta ha salido a la luz porque los materiales procedentes de ella se han utilizado en un proceso penal" (párrafo 351).

5. Principio de legalidad. Reglamentación de los derechos. Control de constitucionalidad. Declaración de inconstitucionalidad. Sistema informático. Vigilancia electrónica.

"La cuestión pertinente en relación con los motivos por los que se puede recurrir a la vigilancia secreta y las personas que pueden ser sometidas a vigilancia es si la ley que autoriza o permite la vigilancia establece con suficiente claridad (a) la naturaleza de los delitos y otros motivos que pueden dar lugar a la vigilancia y (b) las categorías de personas que pueden ser sometidas a vigilancia" (párrafo 298).

"En Bulgaria, la ley establece de manera exhaustiva las infracciones penales dolosas graves que pueden desencadenar el uso de medios especiales de vigilancia. Además, especifica que dichos medios sólo pueden utilizarse si existen motivos para sospechar que se está planeando cometer, se está cometiendo o se ha cometido un delito de este tipo, y sólo si es improbable que otros métodos de detección o investigación tengan éxito. Así pues, la ley es suficientemente clara a este

respecto (véase *Roman Zakharov*). De hecho, es más clara que cuando el Tribunal la examinó por primera vez y la consideró adecuada a este respecto en *Association for European Integration and Human Rights* y *Ekimdzhiev*. Aunque los tipos de delitos que entran en esa lista son variados, parece que en la práctica en la gran mayoría de los casos las autoridades recurren a la vigilancia en relación con los delitos de (a) ser el líder o miembro de una banda criminal y de (b) traficar con estupefacientes" (párrafo 299).

"Es cierto que la ley dice que los medios especiales de vigilancia también pueden utilizarse para ´actividades relacionadas con la seguridad nacional´. A falta de información más detallada sobre la práctica de los tribunales y autoridades búlgaros competentes sobre este punto, es difícil comprobar si, como afirma el Gobierno, la seguridad nacional nunca puede ser un motivo autónomo para la vigilancia en Bulgaria. La exigencia legal de que cada solicitud de vigilancia contenga una exposición completa de las circunstancias que hacen sospechar que se está preparando o cometiendo o se ha cometido un delito relevante, incluso cuando se trata de la seguridad nacional, y la redacción de la disposición que establece el plazo para utilizar medios especiales de vigilancia para proteger la seguridad nacional, que parece vincularla con la prevención de delitos contra la República parecen apoyar la tesis del Gobierno. Sin embargo, sigue sin estar claro cómo se aplican estas disposiciones en la práctica. La falta de claridad sobre este punto ya fue señalada por el Comité de ministros en el contexto de su supervisión de la ejecución de *Asociación para la Integración Europea y los Derechos Humanos* y *Ekimdzhiev*" (párrafo 300).

"Pero incluso si se acepta que, en virtud de la legislación búlgara, la protección de la seguridad nacional puede ser un motivo autónomo para la vigilancia secreta, ello no contraviene en sí mismo el artículo 8 del Convenio (véase *Asociación para la integración europea y los derechos humanos* y *Ekimdzhiev*; *Centrum för rättvisa*; y *Big Brother Watch y otros*). Lo que importa más bien es que puedan controlarse los posibles abusos derivados del significado y los contornos intrínsecamente vagos de la noción de seguridad nacional. Cabe señalar a este respecto que, incluso cuando se trata de seguridad nacional, las autoridades competentes deben solicitar autorización judicial para la vigilancia, lo que puede limitar su discrecionalidad a la hora de interpretar dicha noción y garantizar que existan razones suficientes para someter a alguien a vigilancia en cada caso (véase *Roman Zakharov*). Se trata de una importante salvaguardia contra la arbitrariedad y los abusos [...]" (párrafo 301).

"La ley también establece de manera exhaustiva las categorías de personas u objetos que pueden ser sometidos a vigilancia. Cuando se trata de vigilancia relacionada con infracciones penales, las categorías pertinentes están claramente definidas: se trata de personas sospechosas de cometer infracciones, personas utilizadas involuntariamente para su preparación o comisión, personas que han aceptado ser vigiladas para su propia protección o testigos colaboradores en casos relacionados con una clase limitada de infracciones intencionales graves, así como objetos capaces de conducir a la identificación de dichas personas si se desconoce su identidad. Es cierto que cuando se trata de vigilancia por motivos de seguridad nacional, la ley se expresa en términos más vagos: ´personas u objetos relacionados con la seguridad nacional´. Pero las consideraciones del apartado 301 anterior sobre la posibilidad de controlar los posibles abusos derivados de la vaguedad de la noción de seguridad nacional son igualmente pertinentes en este caso" (párrafo 302).

"[S]urge un problema con la falta de precisión suficiente sobre el significado del término ´objetos´ en el artículo 12(1) de la Ley de 1997. La Ley no aclara si los ´objetos´ que pueden ser sometidos a vigilancia —ya sea porque están relacionados con la seguridad nacional o porque son necesarios para identificar a las personas que deben ser sometidas a vigilancia— tienen que ser concretos (por ejemplo, un local específico, un vehículo específico o una línea telefónica específica). Hay que señalar a este respecto que el régimen de vigilancia secreta en Bulgaria pretende ser un régimen selectivo y no masivo (compárese con *Roman Zakharov*). Aunque se trata de un ejemplo extremo,

el caso de *Mustafa Sezgin Tanrıkulu* ilustra el riesgo de interpretación errónea de disposiciones legales insuficientemente precisas que normalmente están destinadas a permitir únicamente la vigilancia selectiva para permitir en realidad la vigilancia a gran escala. También lo hacen los hechos subyacentes a la condena penal de 2016 de la presidenta del Tribunal de la ciudad de Sofía. En 2014 había autorizado la vigilancia de un sistema automatizado de información policial (que en sí mismo seguramente contenía datos sobre muchas personas), al parecer considerando que ese sistema era un ´objeto´ en el sentido del artículo 12.1 de la Ley de 1997. Posteriormente fue acusada de autorizar la vigilancia de un ´objeto´ que no se ajustaba a la definición legal, pero los tribunales la absolvieron de ese cargo y la declararon culpable únicamente en relación con el plazo de la autorización que había expedido. Aunque, debido a la falta de publicación de las sentencias pertinentes, las razones en las que se basa dicha absolución siguen sin estar claras, ello tiende a sugerir que los tribunales búlgaros no son reacios a interpretar el término ´objetos´ del artículo 12, apartado 1, de la Ley de 1997 de una forma bastante amplia" (párrafo 303).

"[L]la legislación búlgara cumple los requisitos del artículo 8 del Convenio en lo que respecta a los motivos por los que puede recurrirse a la vigilancia secreta y a las personas que pueden ser sometidas a vigilancia, salvo por la falta de una definición más precisa del término ´objetos´ en el artículo 12(1) de la Ley de 1997" (párrafo 304).

"La legislación búlgara establece claramente la duración inicial y máxima de las medidas de vigilancia secreta. También está claro que la vigilancia más allá del período inicialmente autorizado sólo es posible si lo autoriza el juez competente, al que se le debe presentar no sólo una relación completa de los resultados de la vigilancia obtenidos hasta el momento. Por último, la ley establece las circunstancias en las que debe interrumpirse la vigilancia. No obstante, existe un motivo de preocupación: la duración potencial de la autorización inicial de vigilancia por motivos de seguridad nacional, que puede llegar a dos años. La mera duración de ese periodo, unida a los contornos intrínsecamente poco claros de la noción de seguridad nacional, debilita significativamente el control judicial al que debe someterse dicha vigilancia. Este punto ya ha sido señalado por el Comité de ministros en el contexto de su supervisión de la ejecución del caso *Asociación para la Integración Europea y los Derechos Humanos* y *Ekimdzhiev*. Incluso si, como afirma el Gobierno, en la práctica los tribunales nunca emiten tales órdenes por períodos superiores a seis meses, ello no se basa en ninguna limitación legal" (párrafo 305).

6. Principio de proporcionalidad. Democracia. Derechos Humanos. Libertad. Principio de dignidad humana. Política criminal.

"Aunque mejoraron significativamente después de que fueran examinadas por el Tribunal en el asunto *Asociación para la Integración Europea y los Derechos Humanos* y *Ekimdzhiev*, las leyes que rigen la vigilancia secreta en Bulgaria, tal como se aplican en la práctica, siguen sin cumplir las salvaguardias mínimas contra la arbitrariedad y el abuso exigidas en virtud del artículo 8 del Convenio en los siguientes aspectos (a) las normas internas que rigen el almacenamiento y la destrucción del material obtenido a través de la vigilancia no se han hecho accesibles al público; (b) el término ´objetos´ del apartado 1 del artículo 12 de la Ley de 1997 no está definido de forma que garantice que no pueda servir de base para una vigilancia indiscriminada; (c) la excesiva duración de la autorización inicial para la vigilancia por motivos de seguridad nacional —dos años— debilita significativamente el control judicial al que se somete dicha vigilancia; (d) el procedimiento de autorización, tal como funciona en la práctica, no es capaz de garantizar que sólo se recurra a la vigilancia cuando sea ´necesaria en una sociedad democrática´; (e) existen varias lagunas en las disposiciones legales que rigen el almacenamiento, el acceso, el examen, la utilización, la comunicación y la destrucción de los datos de vigilancia; (f) el sistema de supervisión, tal como está organizado actualmente, no cumple los requisitos de independencia, competencia y poderes suficientes; (g) las disposiciones de notificación son demasiado limitadas; y (h) el recurso específico, una reclamación en virtud del artículo 2(1)(7) de la Ley de 1988, no

está disponible en la práctica en todas las situaciones posibles, no garantiza el examen de la justificación de cada caso de vigilancia (por referencia a la sospecha razonable y la proporcionalidad), no está abierto a las personas jurídicas y es limitado en cuanto a las medidas disponibles" (párrafo 356).

"Estas deficiencias del régimen jurídico parecen haber tenido un impacto real en el funcionamiento del sistema de vigilancia secreta en Bulgaria. Los escándalos recurrentes relacionados con la vigilancia secreta sugieren la existencia de prácticas de vigilancia abusivas, que parecen deberse, al menos en parte, a la insuficiencia de las garantías jurídicas (véanse *Asociación para la Integración Europea y los Derechos Humanos* y *Ekimdzhiev* y *Roman Zakharov*) (párrafo 357).

"De ello se desprende que las leyes búlgaras que regulan la vigilancia secreta no cumplen plenamente el requisito de ´calidad de la ley´ y son incapaces de mantener la ´interferencia´ que conlleva el sistema de vigilancia secreta en Bulgaria dentro de lo ´necesario en una sociedad democrática´" (párrafo 358).

"Aunque las leyes que rigen la retención de datos de comunicaciones y su posterior acceso por parte de las autoridades mejoraron significativamente después de que el Tribunal Constitucional las examinara en 2015 a raíz de la sentencia del TJUE en el caso *Digital Rights Ireland y otros*, dichas leyes, tal como se aplican en la práctica, siguen sin ofrecer las garantías mínimas contra la arbitrariedad y el abuso exigidas en virtud del artículo 8 del Convenio en los siguientes aspectos: (a) el procedimiento de autorización no parece capaz de garantizar que las autoridades accedan a los datos de comunicaciones retenidos únicamente cuando ello sea ´necesario en una sociedad democrática´; (b) no se han establecido plazos claros para la destrucción de los datos a los que han accedido las autoridades en el curso de procedimientos penales; (c) no existen normas públicamente disponibles sobre el almacenamiento, acceso, examen, uso, comunicación y destrucción de datos de comunicaciones a los que han tenido acceso las autoridades; (d) el sistema de supervisión, tal como está organizado actualmente, no parece capaz de controlar eficazmente los abusos; (e) las disposiciones de notificación, tal como funcionan actualmente, son demasiado limitadas; y (f) no parece que exista un recurso efectivo" (párrafo 419).

"De ello se deduce que dichas leyes no cumplen plenamente el requisito de ´calidad del Derecho´ y son incapaces de mantener la ´interferencia´ que supone el sistema de retención y acceso a los datos de las comunicaciones en Bulgaria dentro de lo ´necesario en una sociedad democrática´" (párrafo 420).

3. ALCANCE DE REGISTROS Y HALLAZGOS INCIDENTALES EN EVIDENCIA DIGITAL

JURISPRUDENCIA NACIONAL

3.1. CÁMARA DE APELACIONES EN LO PENAL, CONTRAVENCIONAL Y DE FALTAS, SALA I. "SOBRE 128 1 PARR. - DELITOS ATINENTES A LA PORNOGRAFÍA (PRODUCIR/PUBLICAR IMÁGENES PORNOGRÁFICAS C. MENORES 18)". CAUSA N°. 2134/2018. ACTUACIÓN N° 12141374/2018. 26/09/2018.

HECHOS

Una persona había publicado en su cuenta personal del sitio Facebook una amenaza dirigida a una diputada nacional y al jefe de gobierno de la Ciudad Autónoma de Buenos Aires. Por ese motivo, resultó imputada por el delito de amenazas simples. En el marco de ese proceso, se ordenó el allanamiento de su vivienda y el secuestro de todos los dispositivos electrónicos con acceso a internet desde los que se pudiera haber realizado la publicación. De esa manera, se secuestraron dos teléfonos celulares y una CPU. Luego, el representante del Ministerio Público Fiscal solicitó a la División Análisis de Inteligencia Informática de la Superintendencia de Delitos Tecnológicos de la Policía de la Ciudad que realizara un informe pericial sobre los dispositivos. En particular, requirió que se identificara la configuración del usuario denunciado, su correo y la actividad desarrollada en el sitio. También dispuso que se aportara información sobre las cuentas de usuario del sistema operativo y de las utilizadas o accedidas a través de navegadores web, aplicaciones de gestión de correos electrónicos, mensajería instantánea, alojamiento de información en la nube y similares. Por último, solicitó que se determinara si las publicaciones que resultaban objeto de la investigación se encontraban almacenadas en alguno de los dispositivos o cuentas personales. Una vez realizada la pericia, la división interviniente informó que se habían encontrado "imágenes con presuntos desnudos de menores que no son de interés para la presente causa". Este hallazgo fue logrado en base a la utilización de un software específico que busca imágenes referentes a posibles desnudos de menores. Con esa información, la Fiscalía inició una nueva causa. En ese marco, la persona fue imputada por el delito de producción, financiación, comercialización y publicación de pornografía infantil. La defensa planteó la nulidad de la pericia. Sobre ese aspecto, sostuvo que se había excedido el objeto de la medida y que el software utilizado tampoco se correspondía con su objeto. El tribunal no hizo lugar al planteo. Contra esa decisión, la defensa interpuso un recurso de apelación.

DECISIÓN

La Sala I de la Cámara de Apelaciones en lo Penal, Contravencional y de Faltas de la Ciudad Autónoma de Buenos Aires, por mayoría, hizo lugar a la impugnación, revocó la decisión y declaró la nulidad del punto pericial referido al almacenamiento de las publicaciones en alguno de los dispositivos o cuentas (jueces Vázquez y Saez Capel, la jueza Alvaro votó en disidencia).

ARGUMENTOS

1. **Derecho a la intimidad. Orden judicial. Debido proceso. Debida diligencia. Prueba. Prueba digital. Apreciación de la prueba. Prueba de peritos. Telefonía celular.**

"[L]a consagración constitucional de los derechos a la intimidad y la privacidad implica que las intromisiones en esos ámbitos tan fundamentales deben ser ordenadas por el juez competente, y deben estar debidamente fundadas […]".

"Así, los mensajes —SMS, WhatsApp, Telegram, correos electrónicos, etc.—, las fotografías, videos, audios, localizaciones por GPS, búsquedas por la web, intereses, archivos, etc., pueden guardar los aspectos más íntimos de la persona. Tanta información, a su vez, constituye un reservorio importante de prueba que, como tal, debe ser limitado y regulado (El Acceso a Información y Datos de Teléfonos Celulares, Maximiliano Hairabedián, en el libro 'Cibercrimen', editorial IBdeF, 2017)".

"[R]esulta fundamental establecer si la pericia realizada sobre los dispositivos electrónicos de R. R, fue excesiva y constituyó, así, una violación a los derechos mencionados, o bien, si se atuvo a lo ordenado por las autoridades de primera instancia, y resultó razonable y proporcional al delito investigado".

"Esta investigación se inició por una amenaza escrita y publicada en la red social Facebook. En ese contexto, y pese a que el punto ´5´ de la pericia solicitada por la Fiscalía de primera instancia, y autorizada por la *a quo*, solicitaba que se determine 'si las publicaciones que resultan objeto de la presente investigación se encuentran almacenadas en alguno de los dispositivos o cuentas aludidas', considero que no correspondía llevar a cabo una búsqueda irrestricta en los archivos que el imputado pudiera tener almacenados en sus dispositivos electrónicos".

"[L]a utilización de softwares como el ´UFED 4PC de *Cellebrite´* y el ´*Magnet Axiom Examin* versión 1.2.0.6464´, que organizan y filtran archivos audiovisuales que pueden resultar de interés para una investigación criminal, resulta, a nuestro parecer, excesiva y desproporcionada para el objeto de la presente investigación, que se inició por una amenaza dirigida contra Elisa Carrió y Horacio Rodríguez Larreta, que no contenía imágenes, ni se relacionaba de ningún modo con archivos del tipo audiovisual".

"[L]a utilización del programa ´*Griffeyes Analyze´*, especializado, según lo dicho por el perito interviniente, [...] en la búsqueda de imágenes y videos referentes a presuntos desnudos de menores, resulta, —en palabras de la doctrina norteamericana— una 'excursión de pesca', y una violación a la privacidad del imputado que de ningún modo está justificada por la orden de la *a quo*, ni por las características del hecho investigado".

2. Allanamiento. Debida diligencia. Prueba. Apreciación de la prueba.

"[N]o resulta aplicable al caso la doctrina conocida como ´*plain view doctrine´*, extensamente desarrollada por la Corte Suprema de Estados Unidos. De ella se deriva que, en el marco de una medida de prueba legítima, como podría ser el allanamiento de un domicilio, los funcionarios a los que se les haya encomendado no están impedidos de secuestrar elementos demostrativos de la comisión de un delito distinto de aquel por el cual se libró la orden de ingreso, si la existencia de aquellos elementos fue advertida por accidente o a franca o simple vista".

"El descubrimiento de archivos audiovisuales relacionados con la pornografía infantil a través de la utilización, por parte del oficial a cargo de la pericia, de un programa especializado en la búsqueda de imágenes y videos de desnudos de menores, en el marco de una investigación por una amenaza realizada por escrito, no puede, en modo alguno, calificarse como un descubrimiento accidental o —como señalara la magistrada de primera instancia—, como un hallazgo al que el realizador de la pericia haya llegado, espontáneamente, y a través de sus sentidos".

“[S]i bien es cierto que la declaración de invalidez posee carácter excepcional, y que priman los principios de conservación y trascendencia de los actos procesales, en un caso como el que aquí nos convoca, en el que el punto número ´5´ de la pericia realizada por la división policial ha excedido completamente el marco de la investigación, y se ha inmiscuido en ámbitos de la privacidad del encartado que nada tenían que ver con el hecho pesquisado, corresponde declarar su nulidad”.

JURISPRUDENCIA INTERNACIONAL

3.2. TRIBUNAL DE APELACIONES DEL DÉCIMO CIRCUITO DE LOS ESTADOS UNIDOS DE NORTEAMÉRICA, "UNITED STATES V. CAREY" CAUSA N° 98—3077. 14/04/1999.

HECHOS

Un hombre estaba siendo investigado por la presunta tenencia y comercialización de estupefacientes. Tras varias entregas controladas, la policía obtuvo una orden de detención en su contra. Al momento de practicar la detención en el domicilio del hombre, los oficiales advirtieron a simple vista marihuana y dispositivos para fumar, por lo que le solicitaron su consentimiento para registrar su departamento. Tras una discusión con los oficiales, el hombre dio su consentimiento verbal, que luego ratificó por escrito en una comisaría. Con respaldo en este consentimiento, los oficiales regresaron al domicilio y secuestraron algunos estupefacientes y dos computadoras. Las computadoras fueron llevadas a la comisaría y se obtuvo una orden judicial para registrar archivos relacionados con la venta de estupefacientes. Uno de los oficiales identificó varios archivos en formato "JPG" que, al ser abiertos, contenían fotografías con pornografía infantil. Considerando que existía causa probable para continuar explorando los archivos, el detective descargó aproximadamente doscientos cuarenta y cuatro archivos JPG o de imagen. Por estos hechos, el hombre fue acusado de un cargo de posesión de un disco duro de ordenador que contenía tres o más imágenes de pornografía. El acusado acordó declararse culpable de forma condicional [*conditional guilty plea*] y apeló la decisión del tribunal de distrito que había denegado el pedido de supresión del material incautado en su computadora. Para ello, alegó que se había obtenido como resultado de un registro sin orden judicial.

DECISIÓN

El Tribunal de Apelaciones del Décimo Circuito Judicial de los Estados Unidos, hizo lugar al recurso de apelación y revocó lo resuelto.

ARGUMENTOS

1. **Sistema informático. Prueba. Prueba informática. Prueba digital. Orden judicial. Testimonios.**

"La Corte Suprema ha señalado que 'la doctrina de la *plain view* no puede ser utilizada para extender una búsqueda exploratoria general de un objeto a otro hasta que al final surja algo incriminatorio' [...]. La orden obtenida con el propósito específico de registrar las computadoras del acusado sólo permitía el registro de los archivos informáticos en busca de ´nombres, números de teléfono, libros de contabilidad, recibos, direcciones y otras pruebas documentales relativas a la venta y distribución de sustancias controladas´. Así pues, el alcance del registro se circunscribía a las pruebas relacionadas con el tráfico de drogas. El argumento de que los archivos estaban a la vista no es válido porque lo que se incautó fue el contenido de los archivos y no los archivos en sí".

"El caso gira en torno a que cada uno de los archivos que contenían material pornográfico estaban etiquetados como ´JPG´ y la mayoría presentaba un título sexualmente sugerente. Seguramente, después de abrir el primer archivo y ver una imagen de pornografía infantil, el oficial encargado de la búsqueda supo, antes de abrir los demás archivos, lo que significaba la etiqueta. Cuando abrió los archivos posteriores, sabía que no iba a encontrar elementos relacionados con la actividad de drogas como se especificaba en la orden".

“En la audiencia oral, el acusador sugirió que esta situación es similar a la de un oficial que tiene una orden judicial para registrar un archivador que contiene muchos cajones. Aunque cada cajón está etiquetado, tuvo que abrir un cajón para comprobar si la etiqueta era engañosa y si el cajón contenía los objetos de la búsqueda. Si bien el escenario es probable, no es representativo de los hechos de este caso. Este no es un caso en el que el directorio del disco duro contenga archivos con etiquetas ambiguas. No se trata de un caso en el que los agentes tuvieron que abrir cada cajón del expediente antes de descubrir su contenido. Incluso si empleamos la teoría del archivador, el testimonio del detective hace que la analogía sea inapropiada porque afirmó que sabía, o al menos tenía causa probable para saber, que cada cajón estaba debidamente etiquetado y su contenido estaba claramente descrito en la etiqueta”.

“Debido a que este caso involucra imágenes almacenadas en una computadora, la analogía del archivador puede ser inadecuada. ‘Dado que es probable que el almacenamiento electrónico contenga una mayor cantidad y variedad de información que cualquier método de almacenamiento anterior, las computadoras son objetivos tentadores en la búsqueda de información incriminatoria’ [...]. Depender de analogías con contenedores cerrados o archivadores puede llevar a los tribunales a ´simplificar excesivamente un área compleja de las doctrinas de la Cuarta Enmienda e ignorar las realidades del almacenamiento masivo en computadoras modernas´”.

“Alternativamente, los tribunales pueden reconocer que las computadoras a menudo contienen ´documentos entremezclados´. Bajo este enfoque, las fuerzas del orden deben participar en el paso intermedio de clasificar varios tipos de documentos y luego buscar sólo los especificados en una orden judicial. Cuando los agentes encuentran documentos relevantes tan entremezclados con documentos irrelevantes que no es posible clasificarlos en el lugar, los agentes pueden sellar o retener los documentos hasta que un magistrado apruebe las condiciones y limitaciones de una búsqueda adicional entre los documentos. El magistrado debe entonces exigir a los agentes que especifiquen en una orden judicial qué tipo de archivos se buscan”.

“Con las computadoras y los datos bajo su custodia, los agentes encargados de hacer cumplir la ley generalmente pueden emplear varios métodos para evitar buscar archivos del tipo no identificado en la orden: observar los tipos de archivos y títulos enumerados en el directorio, hacer una búsqueda de palabras clave para términos relevantes, o leer partes de cada archivo almacenado en la memoria. En este caso, el detective [...] y el técnico informático enumeraron los archivos en el directorio y también realizaron una búsqueda de palabras clave, pero no utilizaron la información obtenida para limitar su búsqueda a los elementos especificados en la orden, ni obtuvieron una nueva orden que autoriza la búsqueda de pornografía infantil”.

“Debemos concluir que el detective [...] se excedió en el alcance de la orden judicial del caso. Su incautación de las pruebas, en las que se basó la acusación y condena, fue consecuencia de un registro inconstitucional y el tribunal de distrito cometió un error al negar su exclusión”.

3.3. TRIBUNAL DE APELACIONES DEL NOVENO CIRCUITO DE LOS ESTADOS UNIDOS. "UNITED STATES V. COMPREHENSIVE DRUG TESTING". EXPEDIENTE N° 05.10067. 26/8/2009.

HECHOS

En 2002, el gobierno federal inició una investigación sobre *Bay Area Lab Cooperative* (Balco), de la que sospechaba que suministraba esteroides a jugadores profesionales de béisbol. Ese año, la *Major League Baseball Players Association* también firmó un convenio colectivo con la *Major League Baseball* que preveía la realización de controles antidopaje a todos los jugadores. Durante el primer año de vigencia del convenio, se recogían muestras de orina que eran analizadas en busca de sustancias prohibidas. Se les aseguró a los jugadores que los resultados serían anónimos y confidenciales; el objetivo de las pruebas era únicamente determinar si más del cinco por ciento de los jugadores daban positivo, en cuyo caso se realizarían pruebas adicionales en temporadas futuras. La *Comprehensive Drug Testing, Inc.* (CDT), una empresa independiente, administraba el programa y recogía las muestras de los jugadores; las pruebas las realizaba el laboratorio *Quest Diagnostics, Inc*. La CDT conservaba la lista de jugadores y los resultados de sus respectivas pruebas; Quest conservaba las muestras reales con las que se realizaban las pruebas. Durante la investigación de Balco, las autoridades federales tuvieron conocimiento que diez jugadores habían dado positivo en el programa de CDT. El gobierno obtuvo una citación del gran jurado en el Distrito Norte de California para realizar la búsqueda de todos los "registros de pruebas de drogas y especímenes" pertenecientes a las Grandes Ligas de Béisbol en posesión de la CDT. La CDT y los jugadores intentaron negociar un acuerdo de conformidad con el gobierno, pero, al fracasar las negociaciones, solicitaron la anulación de la citación. El día en que se presentó la moción de anulación, el gobierno obtuvo una orden en el Distrito Central de California autorizando el registro de las instalaciones de la CDT en Long Beach. A diferencia de la citación, la orden se limitaba a los registros de los diez jugadores respecto de los cuales el gobierno tenía motivos fundados. Sin embargo, cuando se ejecutó la orden, el gobierno secuestró y revisó rápidamente los registros de las pruebas de drogas de cientos de jugadores de la *Major League Baseball* (y de muchas otras personas). El gobierno también obtuvo una orden del Distrito de Nevada para las muestras de orina en las que se habían realizado las pruebas de drogas que se guardaban en las instalaciones de Quest en Las Vegas. Posteriormente, el gobierno obtuvo órdenes adicionales para los registros en las instalaciones de la CDT en Long Beach y el laboratorio de Quest en Las Vegas. Por último, el gobierno notificó a la CDT y Quest nuevas citaciones en el Distrito Norte de California, exigiendo la presentación de los mismos registros que acababa de secuestrar. La CDT y los jugadores solicitaron en el Distrito Central de California, de conformidad con la Regla Federal de Procedimiento Penal 41(g), la devolución de los bienes secuestrados.

El juez Cooper consideró que el gobierno no había cumplido con los procedimientos detallados en la orden y, sobre esa base y otras, ordenó la devolución de los bienes (orden Cooper). La CDT y los jugadores solicitaron posteriormente en el Distrito de Nevada, de conformidad con la Regla Federal de Procedimiento Penal 41 (g), la devolución de los bienes secuestrados en virtud de las órdenes emitidas por ese tribunal de distrito. El caso fue analizado por el juez Mahan, quien accedió a la petición y ordenó al gobierno que devolviera los bienes secuestrados, con la excepción del material relativo a los diez jugadores de béisbol identificados (orden Mahan). La CDT y los Jugadores finalmente solicitaron en el Distrito Norte de California, de conformidad con la Regla Federal de Procedimiento Penal 17(c), la anulación de la última ronda de citaciones. El caso fue analizado por el Juez Illston. En una resolución oral, el juez Illston anuló las citaciones (Illston Quashal). Los tres jueces expresaron su descontento con la gestión de la investigación por parte del gobierno, y algunos llegaron a acusar al gobierno de manipulación y tergiversación. No obstante, el gobierno apeló las tres órdenes y un panel dividido del tribunal de California revocó

la Orden Mahan y la Illston Quashal, pero (unánimemente) consideró que la apelación de la Orden Cooper era extemporánea.

DECISIÓN

El Tribunal de Apelaciones del Noveno Circuito decidió que el gobierno violó los derechos de la Cuarta Enmienda.

ARGUMENTOS

1. Procedimiento policial. Estupefacientes. Orden judicial. Derecho a la privacidad. Almacenamiento. Prueba. Prueba digital. Prueba electrónica. Allanamiento.

"Al igual que los jueces Cooper e Illston, el juez Mahan determinó que ´[e]l gobierno despreció insensiblemente los derechos constitucionales de los jugadores afectados´. El Juez Mahan también concluyó que el gobierno ´irrazonablemente se negó a seguir los procedimientos establecidos en *United States v. Tamura* al enterarse de que los registros de las pruebas de drogas de los diez atletas nombrados en las órdenes originales del 8 de abril ejecutadas en Quest y en [CDT] estaban entremezclados con los registros de otros atletas no nombrados en esas órdenes´. Podemos confirmar estas conclusiones basándonos en el efecto preclusivo de las órdenes Cooper e Illston. Sin embargo, porque el asunto es importante, y para evitar cualquier disputa sobre el alcance apropiado de la preclusión, también nos deshacemos de los argumentos contrarios del gobierno".

"El objetivo de los procedimientos del caso *Tamura* es mantener la privacidad de los materiales que se entremezclan con materiales incautables y evitar que una búsqueda limitada de información concreta se convierta en una búsqueda general de los sistemas de archivos de oficina y las bases de datos informáticas. Si el gobierno no puede estar seguro de si los datos pueden estar ocultos, comprimidos, borrados o contener trampas sin examinar cuidadosamente el contenido de cada archivo, entonces todo lo que el gobierno decida secuestrar quedará automáticamente a la vista, según esta teoría".

"Dado que los agentes del gobierno deciden en última instancia cuánto secuestrar, esto creará un poderoso incentivo para que incauten más en lugar de menos: ¿Por qué detenerse en la lista de todos los jugadores de béisbol cuando se puede secuestrar todo el Directorio Tracey? ¿Por qué sólo ese directorio y no todo el disco duro? ¿Por qué sólo este ordenador y no el de la habitación de al lado y el de la habitación de al lado? ¿No encuentras el ordenador? Confisque los discos Zip bajo la cama en la habitación donde podría haber estado el ordenador. Véase *United States v. Hill*. Llevémoslo todo al laboratorio, echemos un buen vistazo y veamos con qué podemos tropezar. Esto sería una burla a la regla del caso *Tamura* y anularía las garantías cuidadosamente elaboradas en la orden judicial del Distrito Central".

"Este caso ilustra bien tanto los retos a los que se enfrentan las fuerzas del orden modernas a la hora de recuperar la información que necesitan para perseguir y procesar a los malhechores, como la amenaza que supone para la intimidad de las partes inocentes una investigación penal enérgica. En la época del caso *Tamura*, la mayoría de los particulares y empresas guardaban sus archivos en archivadores o instalaciones físicas similares. Hoy en día, el mismo tipo de datos suele almacenarse electrónicamente, a menudo lejos de las instalaciones. Las instalaciones de almacenamiento electrónico entremezclan los datos, lo que dificulta su recuperación sin un conocimiento profundo de los sistemas de archivo y clasificación utilizados, algo que a menudo sólo puede determinarse analizando detenidamente los datos en un entorno controlado. En el caso *Tamura* se afectó a unas pocas docenas de cajas y se consideró una incautación amplia; pero

incluso los medios de almacenamiento electrónico de bajo coste pueden almacenar hoy en día el equivalente a millones de páginas de información".

"Los delincuentes y sus colaboradores tienen incentivos obvios para dificultar la localización de datos, pero las partes implicadas en actividades lícitas también pueden cifrar o comprimir datos por razones totalmente legítimas: protección de la intimidad, preservación de comunicaciones privilegiadas, defensa contra el espionaje industrial o prevención de delitos generales como la usurpación de identidad. Así pues, hoy en día las fuerzas de seguridad tienen una tarea mucho más difícil, exigente y delicada a la hora de buscar pruebas de actividades delictivas que incluso en un pasado relativamente reciente. A menudo hemos reconocido la necesidad legítima de recoger grandes cantidades de datos y examinarlos cuidadosamente en busca de pruebas ocultas o encubiertas. Véase, por ejemplo, *United States v. Hill*".

"En este caso, por ejemplo, la solicitud de orden judicial presentada al juez Johnson hablaba de los numerosos riesgos teóricos de que los datos pudieran ser destruidos, pero no mencionaba que *Comprehensive Drug Testing* había accedido a conservar los datos intactos hasta que el tribunal de distrito del norte de California pudiera pronunciarse sobre su petición de anulación de la citación, y que la Fiscalía de los Estados Unidos había aceptado esta declaración. Esta omisión creó la falsa impresión de que, a menos que los datos se secuestran de inmediato, se perderían. Tales promesas de conservación de datos son obviamente muy importantes para determinar si se necesita una orden judicial y, en caso afirmativo, cuál debe ser su alcance. Si el Gobierno considera que esas garantías no son fiables, puede decirlo y explicar por qué. Pero omitir por completo una información tan relevante es incompatible con el deber de franqueza del gobierno al presentar una solicitud de orden judicial. La falta de franqueza en este o en cualquier otro aspecto de la solicitud de orden judicial pesará en contra del gobierno en el cálculo de cualquier moción posterior para devolver o suprimir los datos incautados".

"Por último, el proceso de clasificar, segregar, descodificar y separar de cualquier otro modo los datos incautables (tal como se definen en la orden) del resto de datos debe estar diseñado para lograr ese fin y sólo ese fin. Por lo tanto, si se permite al gobierno hacerse de información relativa a diez nombres, el protocolo de búsqueda debe estar diseñado para descubrir los datos relativos a esos nombres solamente, no a otros, y no los relativos a otra ilegalidad. Por ejemplo, el gobierno dispone de sofisticadas herramientas de *hash* que permiten identificar archivos ilegales bien conocidos (como pornografía infantil) sin necesidad de abrir los propios archivos. Estas herramientas de búsqueda y otras similares no pueden utilizarse sin una autorización específica en la orden judicial, y dicha autorización sólo puede concederse si existe causa probable para creer que dichos archivos pueden encontrarse en el soporte electrónico que se va a secuestrar".

"Esta necesidad acuciante de las fuerzas de seguridad de una autorización amplia para examinar registros electrónicos, tan persuasivamente demostrada en la introducción de la orden original en este caso [...] crea un grave riesgo de que toda orden de información electrónica se convierta, de hecho, en una orden general, haciendo irrelevante la Cuarta Enmienda. El problema puede plantearse de forma muy sencilla: no hay forma de saber exactamente qué contiene un archivo electrónico sin examinar su contenido de alguna manera, ya sea abriéndolo y mirándolo, utilizando software forense especializado, buscando palabras clave o alguna otra técnica similar".

"Pero los archivos electrónicos suelen encontrarse en soportes que también contienen miles o millones de otros archivos entre los que pueden estar almacenados u ocultos los datos buscados. Por necesidad, los esfuerzos del gobierno por localizar archivos concretos requerirán examinar muchos otros archivos para excluir la posibilidad de que los datos buscados estén ocultos en ellos".

"[U]na vez examinado un archivo, el gobierno puede alegar (como hizo en este caso) que su contenido está a la vista y, si es incriminatorio, el gobierno puede quedárselo. Por lo tanto, la autorización para registrar algunos archivos informáticos se convierte automáticamente en autorización para registrar todos los archivos del mismo subdirectorio, y todos los archivos de un directorio adyacente, un disco duro vecino, un ordenador cercano o un medio de almacenamiento cercano. Cuando los ordenadores no están cerca unos de otros, pero están conectados electrónicamente, la búsqueda original podría justificar el examen de archivos en ordenadores situados a muchos kilómetros de distancia, basándose en la teoría de que los datos electrónicos incriminatorios podrían haber sido transportados y ocultados allí".

"La aparición de redes rápidas y baratas ha hecho posible almacenar información en ubicaciones remotas de terceros, donde se entremezcla con la de otros usuarios. Por ejemplo, muchas personas ya no guardan su correo electrónico principalmente en su ordenador personal, sino que utilizan un proveedor de correo electrónico basado en la web, que almacena sus mensajes junto con miles de millones de mensajes de y para millones de otras personas. Existen servicios similares para fotografías, presentaciones de diapositivas, código informático y muchos otros tipos de datos. Como resultado, las personas tienen ahora datos personales que se almacenan con los de innumerables desconocidos. La incautación, por ejemplo, de los servidores de correo electrónico de Google para buscar unos pocos mensajes incriminatorios podría poner en peligro la privacidad de millones de personas".

"No es una respuesta sugerir, como hizo la mayoría del panel de tres jueces [de distrito], que la gente puede evitar estos peligros no almacenando sus datos electrónicos. Para empezar, la decisión sobre cómo se almacena la información suele tomarla alguien que no es la persona cuya intimidad se vería invadida por la búsqueda. La mayoría de la gente no tiene ni idea de si su médico, su abogado o su contable guardan sus expedientes en papel o en formato electrónico, si se almacenan en sus instalaciones [...], si se mezclan con los de muchos otros profesionales o se mantienen totalmente separados. En este caso, por ejemplo, el directorio de Tracey contenía un gran número de registros de pruebas antidopaje, no sólo de los diez jugadores para los que el gobierno tenía una causa probable, sino de cientos de otros jugadores profesionales de béisbol, otras trece organizaciones deportivas, tres competiciones deportivas no relacionadas y una entidad comercial no deportiva: miles de archivos en total, que reflejaban los resultados de las pruebas de un número desconocido de personas, la mayoría sin relación con el béisbol profesional, excepto que tuvieron la mala suerte de que los resultados de sus pruebas se almacenarán en el mismo ordenador que los jugadores de béisbol".

2. Derecho a la privacidad. Derecho a la intimidad. Prueba informática. Prueba digital. Orden judicial. Razonabilidad. Protección de datos personales. Procedimiento policial.

"En segundo lugar, almacenar los datos electrónicamente tiene ventajas muy importantes. Poder hacer copias de seguridad de los datos y evitar la pérdida por incendio, inundación o terremoto es una de ellas. La facilidad de acceso desde lugares remotos mientras se viaja es otra. La capacidad de compartir rápidamente los datos entre profesionales, como el envío de resonancias magnéticas para su examen por un especialista en cáncer al otro lado del mundo, puede significar la diferencia entre la muerte y una recuperación completa. El almacenamiento y la transmisión electrónicos de datos ya no son una peculiaridad o un lujo de los muy ricos; son una forma de vida".

"Las intrusiones gubernamentales en grandes bases de datos privadas pueden exponer información extremadamente sensible sobre innumerables personas no implicadas en ninguna actividad delictiva, que podrían incluso no saber que se ha confiscado información sobre ellas y, por tanto, no pueden hacer nada para proteger su intimidad".

“No es de extrañar, por tanto, que los tres jueces de distrito se mostraron muy preocupados por la conducta del gobierno en este caso. El juez Mahan, por ejemplo, preguntó ´¿qué ha sido de la Cuarta Enmienda? ¿Fue derogada de alguna manera?´. El juez Cooper se refirió a ´la imagen de mover rápida y hábilmente la taza para que nadie pueda encontrar el guisante´. Y el Juez Illston consideró las tácticas del gobierno como ´irrazonables´ y encontró que constituían ´acoso´. También el juez Thomas, en su voto particular discrepante, expresó su frustración por la conducta y la postura del gobierno, calificándola de ´expansión impresionante de la doctrina de la ´vista sin obstáculos´, que claramente no tiene aplicación a los datos electrónicos privados entremezclados´”.

“Los intereses de todos están mejor servidos si existen normas claras a seguir que establezcan un equilibrio justo entre las necesidades legítimas de la aplicación de la ley y el derecho de las personas y las empresas a la intimidad, que es el núcleo de la Cuarta Enmienda. El caso *Tamura* ha proporcionado un marco viable durante casi tres décadas, y bien podría haber bastado en este caso si se hubieran seguido sus enseñanzas. Creemos que es útil, por lo tanto, actualizar la regla del caso *Tamura* para aplicarlo a las desalentadoras realidades de los registros electrónicos que casi siempre presentarán el tipo de situación que el caso *Tamura* creía que sería rara y excepcional: la incapacidad de los agentes del gobierno para separar los materiales incautables de los no incautables en el lugar del registro y, por lo tanto, la necesidad de secuestrar mucho más de lo que realmente está autorizado”.

“Aceptamos la realidad de que este tipo de incautación excesiva es una parte inherente del proceso de búsqueda electrónica y partimos del supuesto de que, cuando se trata de la incautación de registros electrónicos, esto será mucho más común que en los días de los registros en papel. Esto exige una mayor vigilancia por parte de los funcionarios judiciales a la hora de encontrar el equilibrio adecuado entre el interés del gobierno en la aplicación de la ley y el derecho de las personas a no ser objeto de registros e incautaciones irrazonables. El proceso de separar los datos electrónicos que son incautables de los que no lo son no debe convertirse en un vehículo para que el gobierno acceda a datos que no tiene causa probable para recoger. En general, adoptamos la solución del caso *Tamura* al problema de la necesaria incautación excesiva de pruebas: cuando el gobierno desea obtener una orden judicial para examinar el disco duro de un ordenador o un medio de almacenamiento electrónico en busca de determinados archivos incriminatorios, o cuando una búsqueda de pruebas podría dar lugar a la incautación de un ordenador, véase, por ejemplo, *United States v. Giberson*, los jueces de instrucción deben estar atentos para observar las orientaciones que hemos expuesto a lo largo de nuestra opinión, que pueden resumirse de la siguiente manera:

1. Los magistrados deben insistir en que el gobierno renuncie a la doctrina del *plain view* en los casos de pruebas digitales.

2. La segregación y la redacción deben correr a cargo de personal especializado o de un tercero independiente. Si la segregación va a ser realizada por personal informático de la Administración, ésta debe acordar en la solicitud de orden que el personal informático no revelará a los investigadores ninguna información distinta de la que es objeto de la orden.

3. Las órdenes judiciales y las citaciones deben revelar los riesgos reales de destrucción de la información, así como los esfuerzos previos por hacerse de esa información en otros foros judiciales.

4. El protocolo de registro del gobierno debe estar diseñado para descubrir sólo la información para la que tiene causa probable, y sólo esa información puede ser examinada por los agentes del caso.

5. El gobierno debe destruir o, si el destinatario puede poseerlos legalmente, devolver los datos que no respondan, manteniendo informado al magistrado emisor sobre cuándo lo ha hecho y qué ha conservado".

"Al igual que en el caso *Tamura* ha servido de guía durante décadas, confiamos en que los procedimientos que hemos esbozado anteriormente resulten una herramienta útil para el futuro. Al final, sin embargo, debemos confiar en el buen sentido y la vigilancia de nuestros jueces y magistrados, que están en primera línea para preservar las libertades constitucionales de nuestros ciudadanos al tiempo que ayudan al gobierno en sus esfuerzos legítimos para perseguir la actividad criminal. Nada de lo que digamos podría sustituir el buen juicio que los funcionarios judiciales deben ejercer para lograr este delicado equilibrio".

4. MONITOREO E INTERCEPTACIONES ELECTRÓNICAS. REGISTRO REMOTO DE SISTEMAS INFORMÁTICOS

JURISPRUDENCIA INTERNACIONAL

4.1. TRIBUNAL CONSTITUCIONAL FEDERAL DE ALEMANIA. SENTENCIA DEL PRIMER SENADO. "DIE LINKE". CAUSA N° 370/07. 27/02/2008.

HECHOS

Tres abogados y una periodista, miembro del partido de izquierda (*Die Linke*) de Renania del Norte-Westfalia, impulsaron una acción judicial contra las disposiciones de la Ley de Protección de la Constitución del Estado Federal. La normativa autorizaba a los servicios de inteligencia, en su labor de lucha contra el terrorismo, a llevar a cabo acciones como el monitoreo e intercepción de datos en tiempo real de comunicaciones electrónicas y el "registro remoto" de sistemas informáticos mediante el uso de software malicioso (*malware*), especialmente a través de una clase de malware conocida como "troyanos". Los demandantes argumentaron que estas prácticas de los servicios de inteligencia comprometían la confidencialidad e integridad de los sistemas de tecnología de la información. Por su parte, el Estado provincial sostuvo que el debate debería centrarse en el derecho a la privacidad de las telecomunicaciones, mientras que el Estado federal argumentó que la disputa debía encuadrarse en el ámbito de la garantía de inviolabilidad del domicilio.

DECISIÓN

El Tribunal Constitucional Alemán resolvió que la recolección de datos sobre cuentas y transacciones bancarias constituye una interferencia en el derecho a la personalidad, entendido como derecho a la autodeterminación informativa.

ARGUMENTOS

1. Derecho a la privacidad. Protección de datos personales. Sistema informático. Vigilancia electrónica. Identificación de personas. Principio de legalidad. Control judicial. Control de constitucionalidad. Principio de proporcionalidad. Sistema informático. Medidas de seguridad. Informe pericial. Vigilancia electrónica. Fuerzas de seguridad. Derecho a la autodeterminación informativa.

"El derecho fundamental a la protección de la integridad y confidencialidad de los sistemas de tecnología de la información es aplicable cuando la base legal que autoriza las injerencias abarca sistemas que pueden contener, por sí mismos o debido a conexiones de red, datos personales de los usuarios en cantidades tan grandes y de tal variedad que el acceso al sistema facilita el conocimiento de aspectos esenciales de la vida personal o incluso permite crear un perfil completo de la personalidad. Estas posibilidades existen, por ejemplo, cuando se accede a computadoras personales, independientemente de que estén instalados en un lugar fijo o funcionen como dispositivos móviles. En lo que respecta tanto al uso privado como profesional de las computadoras, los patrones de uso permiten extraer regularmente conclusiones sobre las características o preferencias personales. Además, la protección específica de los derechos fundamentales abarca también los teléfonos móviles o dispositivos electrónicos que ofrecen una amplia gama de funciones y pueden recoger y almacenar diversos tipos de datos personales".

"El derecho fundamental a la protección de la confidencialidad e integridad de los sistemas de tecnología de la información protege principalmente el interés del usuario en la confidencialidad

de los datos creados, procesados y almacenados por los sistemas de tecnología de la información que entran dentro de su ámbito de protección. Además, constituye una injerencia en este derecho fundamental el hecho de que la integridad del sistema de tecnología de la información protegido se vea comprometida porque se acceda al sistema de una manera que permita a terceros utilizar sus servicios, funciones y contenidos de almacenamiento; dicho acceso es el paso técnico crítico que permite realizar actividades de espionaje, vigilancia o manipulación en relación con este sistema".

"En su manifestación aquí abordada, el derecho general de la personalidad ofrece protección en particular contra el acceso encubierto mediante el cual los datos disponibles en el sistema pueden ser espiados en su totalidad o a gran escala. Esta protección del derecho fundamental se extiende tanto a los datos almacenados en la memoria de trabajo como a los datos conservados temporal o permanentemente en los soportes de almacenamiento del sistema. El derecho fundamental también protege contra la recogida de datos realizada por medios que, aunque no estén directamente relacionados a nivel técnico con las actividades de tratamiento de datos del sistema informático en cuestión, sin embargo, pertenecen al tratamiento de datos del sistema. Esto se aplica, por ejemplo, al uso de los llamados *keyloggers* de *hardware* o a la medición de la radiación electromagnética de monitores o teclados".

"La expectativa de confidencialidad e integridad goza de la protección de los derechos fundamentales independientemente de si se puede acceder fácilmente al sistema informático o sólo con un esfuerzo considerable. Sin embargo, la expectativa de confidencialidad e integridad sólo se reconoce desde la perspectiva de los derechos fundamentales en la medida en que el usuario afectado considere el sistema de tecnología de la información como su propio sistema, de modo que pueda esperar legítimamente que, en función de las circunstancias pertinentes, tenga control sobre el sistema de tecnología de la información de manera autodeterminada, ya sea solo o junto con otros usuarios autorizados del sistema. [...]".

"El derecho fundamental a la protección de la confidencialidad e integridad de los sistemas informáticos no está garantizado sin limitaciones. Las interferencias pueden estar justificadas tanto para prevenir [peligros para la seguridad pública] como para fines policiales. Los particulares sólo deben aceptar aquellas restricciones de su derecho que tengan una base legal acorde con el derecho constitucional. La disposición que autoriza a la Oficina del Estado local para la Protección de la Constitución a llevar a cabo medidas preventivas, que está siendo revisada en el presente procedimiento, no cumple este requisito".

"El requisito de especificidad jurídica se basa en el principio del Estado de Derecho (artículos 20 y 28(1) de la Ley Fundamental), incluso cuando se refiere al derecho general de la personalidad en sus diversas manifestaciones. Sirve para garantizar que el legislador, legitimado democráticamente, tome por sí mismo las decisiones esenciales sobre las injerencias en los derechos fundamentales y su alcance; que la ley someta al Gobierno y a la Administración a normas que dirijan y limiten su actuación; y que los tribunales puedan controlar la legalidad de sus actos. Además, unas disposiciones claras y específicas garantizan que las personas afectadas puedan discernir la ley aplicable y puedan tomar precauciones contra medidas potencialmente intrusivas. El legislador debe especificar, de forma suficientemente clara y precisa y para cada materia, los motivos, la finalidad y los límites de la injerencia".

"Sobre la base de estas normas, el artículo 5, apartado 2, número 11, primera frase, segunda alternativa, de la Ley de protección de la Constitución de Renania del Norte-Westfalia no cumple el requisito de claridad y especificidad jurídicas en la medida en que las condiciones en las que las medidas son permisibles no pueden deducirse de la disposición legal con suficiente certeza".

“Las condiciones legales para llevar a cabo medidas con arreglo al artículo 5, apartado 2, número 11, primera frase, segunda alternativa, de la Ley de protección de la Constitución de Renania del Norte-Westfalia vienen determinadas por dos referencias a otras disposiciones. En primer lugar, el artículo 5(2) de la Ley de protección de la Constitución de Renania del Norte-Westfalia contiene una referencia general al artículo 7(1) de la Ley de protección de la Constitución de Renania del Norte-Westfalia, que a su vez remite al artículo 3(1) de la Ley de protección de la Constitución de Renania del Norte-Westfalia. Estas disposiciones autorizan el uso de métodos de los servicios de inteligencia con el fin de recabar información relevante para la protección del orden constitucional. En segundo lugar, el artículo 5, apartado 2, número 11, segunda frase, de la Ley de protección de la Constitución de Renania del Norte-Westfalia hace referencia a los requisitos más estrictos establecidos en la Ley sobre el artículo 10 de la Ley Fundamental (en lo sucesivo, la Ley del artículo 10) para los casos en que una medida con arreglo al artículo 5, apartado 2, número 11, de la Ley de protección de la Constitución de Renania del Norte-Westfalia interfiera en la intimidad de la correspondencia, el correo y las telecomunicaciones o sea equivalente a tal interferencia debido a su naturaleza y gravedad”.

“No es compatible con el requisito de claridad y especificidad jurídicas que el artículo 5, apartado 2, número 11, segunda frase, de la Ley de protección de la Constitución de Renania del Norte-Westfalia supedite la aplicabilidad de la Ley del artículo 10 a si una medida interfiere con el artículo 10 de la Ley Fundamental. [...] El uso legislativo de una cláusula de separabilidad (*salvatorische Klausel*) no satisface el requisito de especificidad jurídica de una disposición como el artículo 5, apartado 2, número 11, primera frase, segunda alternativa, de la Ley de protección de la Constitución de Renania del Norte-Westfalia, que prevé nuevas medidas de investigación diseñadas en respuesta a los nuevos avances tecnológicos”.

“La violación del requisito de claridad jurídica se ve agravada por la segunda frase del apartado 2 del artículo 5 número 11 de la Ley de protección de la Constitución de Renania del Norte-Westfalia, que establece además que la Ley del artículo 10 también se aplica si la ´naturaleza y gravedad´ de una medida de investigación equivale a una injerencia en el artículo 10 de la Ley Fundamental. Por lo tanto, las condiciones en las que se permite el acceso [a los sistemas de tecnología de la información] en virtud de la disposición impugnada están supeditadas a una evaluación en la que se compare la medida de acceso con una medida que se calificaría de injerencia en un derecho fundamental específico. El artículo 5, apartado 2, número 11, segunda frase, de la Ley de protección constitucional de Renania del Norte-Westfalia carece por completo de criterios para llevar a cabo dicha comparación. [...]”.

“Además, la referencia al artículo 10 de la Ley en el artículo 5, apartado 2, número 11, segunda frase, de la Ley de protección de la Constitución de Renania del Norte-Westfalia no cumple el requisito de claridad y especificidad jurídicas en la medida en que su alcance no es suficientemente claro”.

“El artículo 5, apartado 2, número 11, primera frase, segunda alternativa, de la Ley de Protección de la Constitución de Renania del Norte-Westfalia tampoco cumple el principio de proporcionalidad. Este principio exige que una injerencia en los derechos fundamentales responda a una finalidad legítima y sea adecuada, necesaria y apropiada para alcanzar dicha finalidad”.

“Las medidas de recogida de datos previstas en la disposición impugnada tienen por objeto ayudar a la Oficina del *Land* para la Protección de la Constitución en el cumplimiento de sus funciones [...], y sirven así para proteger, como medidas cautelares antes de que surjan peligros concretos (*konkrete Gefahren*), el orden básico democrático libre, la existencia de la Federación y de los

Länder, así como los intereses de la República Federal de Alemania que conciernen a sus relaciones internacionales".

"La seguridad del Estado como poder constituido de paz y orden, así como la seguridad de la población a la que está obligado a proteger contra los peligros para la vida, la integridad física y la libertad, tienen el mismo rango que otros valores constitucionales a los que se concede un alto rango. El deber de protección [del Estado] se desprende tanto del artículo 2(2) primera frase y del artículo 1(1) segunda frase de la Ley Fundamental. Al contrarrestar los peligros de actividades terroristas o de otro tipo, el Estado cumple su mandato constitucional. El creciente uso de medios de comunicación electrónicos o digitales y su avance en prácticamente todos los ámbitos de la vida ha creado nuevos obstáculos para el desempeño eficaz de las tareas de la Oficina de Protección de la Constitución. Las modernas tecnologías de la información también ofrecen a los grupos extremistas y terroristas numerosas posibilidades para establecer y mantener contactos, así como para planificar, preparar y cometer actos delictivos. En particular, las medidas legislativas que permiten que las investigaciones estatales se centren en la tecnología de la información deben considerarse en el contexto del cambio de las formas tradicionales de comunicación a la mensajería electrónica y las posibilidades de cifrar u ocultar archivos de datos".

"El acceso encubierto a los sistemas informáticos es idóneo para lograr estos fines. Amplía las posibilidades de que dispone la Oficina de Protección de la Constitución para investigar amenazas. Se concede al legislador un margen de apreciación considerable a la hora de evaluar la idoneidad de una medida".

"Además, el acceso encubierto a los sistemas de tecnología de la información no vulnera el requisito de necesidad. Entraba dentro de la prerrogativa de apreciación del legislador presumir que no se dispone de otros medios para la recogida de datos del sistema de tecnología de la información que sean igualmente eficaces, pero menos intrusivos para las personas afectadas".

"Sin embargo, el artículo 5(2) número 11 primera frase, segunda alternativa de la Ley de Protección de la Constitución de Renania del Norte-Westfalia no cumple el requisito de proporcionalidad en sentido estricto. El principio de proporcionalidad en sentido estricto exige que la gravedad de la injerencia, en una valoración global, no sea desproporcionada en relación con el peso de las razones invocadas para justificarla. El legislador debe sopesar adecuadamente el interés individual que se ve mermado por una injerencia en los derechos fundamentales frente a los intereses públicos perseguidos. Una evaluación basada en estas normas puede llevar a la conclusión de que determinados medios no deben utilizarse para hacer cumplir los intereses públicos porque los perjuicios resultantes para los derechos fundamentales son superiores a los intereses perseguidos".

"El artículo 5, apartado 2, número 11, primera frase, segunda alternativa, de la Ley de protección de la Constitución de Renania del Norte-Westfalia no cumple este requisito. Las medidas previstas en dicha disposición dan lugar a injerencias en los derechos fundamentales tan graves que resultan desproporcionadas en relación con el interés público de investigación que motiva la injerencia. Además, serían necesarias garantías procesales adicionales para hacer efectivos los intereses de derechos fundamentales protegidos de las personas afectadas; éstas también faltan en la disposición".

"El artículo 5, apartado 2, número 11, primera frase, segunda alternativa, de la Ley de protección de la Constitución de Renania del Norte-Westfalia autoriza injerencias especialmente intrusivas en los derechos fundamentales".

“Cuando el Estado recopila datos de sistemas informáticos complejos, existe un potencial considerable de que los datos puedan utilizarse para espiar la personalidad de las personas afectadas. Esto ya se aplica a las medidas que sólo implican un acceso único y aislado, como la incautación o copia de los medios de almacenamiento del sistema”.

“Este acceso encubierto a los sistemas de tecnología de la información proporciona a la autoridad estatal competente acceso a registros de datos que, por su volumen y variedad, pueden superar con creces las fuentes tradicionales de información. Esto se deriva del hecho de que los complejos sistemas de tecnología de la información permiten muchos usos posibles diferentes que implican la creación, el tratamiento y el almacenamiento de datos personales. Habida cuenta de los hábitos actuales de los usuarios, estos dispositivos suelen utilizarse también para almacenar deliberadamente datos personales especialmente sensibles, por ejemplo, documentos de texto privados, imágenes o archivos de sonido. Estos registros de datos pueden incluir información detallada sobre las circunstancias personales y la vida privada de la persona afectada, su correspondencia privada y profesional a través de diversos canales de comunicación, o incluso notas personales a modo de diario”.

“El acceso del Estado a registros de datos tan completos conlleva el riesgo evidente de que, en una evaluación global, los datos recopilados permitan extraer conclusiones exhaustivas sobre la personalidad del afectado, que pueden incluir incluso la creación de perfiles de comportamiento y comunicación”.

“En la medida en que los datos recogidos proporcionan información sobre las comunicaciones entre la persona afectada y terceros, la gravedad de la injerencia en los derechos fundamentales se agrava aún más, dado que restringe la libertad de los ciudadanos de participar en las telecomunicaciones sin ser vigilados, libertad que también sirve al bien común [...]. Además, tales medidas de recogida de datos afectan indiscriminadamente a un número considerable de personas, lo que aumenta el peso de la injerencia, ya que necesariamente afectan también a los interlocutores de comunicación de la persona objeto de la medida, es decir, a terceros, independientemente de si los motivos legales para tal acceso a los datos se cumplen también en relación con estos terceros (en relación con la vigilancia de las telecomunicaciones)”.

“La injerencia en los derechos fundamentales es especialmente grave si —como prevé la disposición impugnada— la infiltración técnica encubierta permite una vigilancia a más largo plazo del uso del sistema y la recogida continua de los datos pertinentes”.

“El volumen y la variedad de los registros de datos que pueden obtenerse mediante un acceso de este tipo son considerablemente mayores que en el caso de medidas puntuales y aisladas de recopilación de datos. Al acceder al sistema objetivo, la autoridad investigadora también obtiene datos volátiles que sólo se conservan en la memoria de trabajo, o datos almacenados sólo temporalmente en los medios de almacenamiento del sistema objetivo. También permite rastrear toda la comunicación por Internet de la persona afectada durante un período más largo. Además, los efectos indiscriminados de la medida de investigación pueden aumentar si el acceso se extiende a una red (local) de la que forme parte el sistema objetivo”.

“Los datos volátiles o almacenados sólo temporalmente pueden tener vínculos especialmente estrechos con la personalidad de las personas afectadas; también pueden facilitar el acceso a otros datos, especialmente sensibles. Esto se aplica, por ejemplo, a los datos de caché, creados por aplicaciones informáticas como los navegadores web; su análisis puede proporcionar información sobre cómo se utilizan dichas aplicaciones y, por tanto, permitir extraer indirectamente conclusiones sobre las preferencias o pautas de comunicación de los usuarios. Lo mismo ocurre con las contraseñas, que permiten al usuario acceder a contenidos técnicamente

seguros de su sistema o de la red. Además, la vigilancia a largo plazo de las comunicaciones por Internet, tal como autoriza la disposición impugnada, es una injerencia considerablemente más intrusiva que una recogida puntual de datos sobre el contenido y las circunstancias de las comunicaciones. Por último, debe tenerse en cuenta que las posibilidades de acceso establecidas en la disposición impugnada sirven, entre otras cosas, para eludir el uso de la tecnología de cifrado y constituyen medios adecuados a este respecto. De este modo, se menoscaban las precauciones individuales adoptadas por los usuarios para protegerse contra el acceso no deseado a los datos. La frustración de la autoprotección informativa emprendida por los afectados aumenta la gravedad de la injerencia en sus derechos fundamentales".

"Además, existe un mayor riesgo de que esto conduzca a la creación de perfiles de comportamiento y comunicación, dado que la disposición autoriza el seguimiento exhaustivo del uso del sistema objetivo durante un período más largo. Por estos medios, la autoridad estatal competente puede espiar ampliamente las circunstancias personales y el comportamiento comunicativo de las personas afectadas. Esta recopilación exhaustiva de datos personales supone una injerencia especialmente intrusiva en los derechos fundamentales".

"La gravedad de la injerencia derivada del acceso [a los sistemas de tecnología de la información], tal como se establece en la Ley, se deriva además del carácter encubierto de la medida. En un Estado de Derecho, las injerencias estatales a través de medidas encubiertas son la excepción y requieren una justificación especial. Si las personas afectadas conocen una medida estatal que les afecta antes de su ejecución, pueden defender sus intereses desde el principio. En primer lugar, pueden tomar medidas legales para impedirla, por ejemplo, recurriendo a un tribunal. En segundo lugar, cuando las medidas de recogida de datos se llevan a cabo abiertamente, pueden influir realmente con su conducta en el curso de la investigación. Excluir esta posibilidad de influir en la investigación aumenta el peso de la injerencia en los derechos fundamentales (cf. en relación con las posibilidades de defensa jurídica)".

"El peso de la injerencia también viene informado por los posibles riesgos para la integridad del ordenador accedido y para los intereses jurídicos de las personas afectadas, o incluso de terceros, que puedan derivarse de dicho acceso".

"Habida cuenta de su gravedad, la injerencia en los derechos fundamentales derivada del acceso encubierto a sistemas informáticos con fines de prevención sólo es procedente si los hechos concretos indican un peligro inminente (*drohende Gefahr*) para un interés jurídico excepcionalmente relevante en el caso concreto; este requisito puede cumplirse incluso si aún no puede establecerse con suficiente probabilidad que el peligro se materializará en un futuro próximo. Además, la disposición legal que autoriza tal injerencia debe garantizar la protección de los derechos fundamentales de las personas afectadas, incluso mediante garantías procesales adecuadas".

"En lo que respecta a la tensión entre el deber del Estado de garantizar la protección de los intereses jurídicos y el interés del individuo en mantener sus derechos constitucionalmente garantizados, corresponde en primer lugar al legislador lograr un equilibrio abstracto entre los intereses en conflicto. En consecuencia, algunas injerencias especialmente intrusivas en los derechos fundamentales sólo pueden permitirse para la protección de determinados intereses jurídicos y únicamente cuando la sospecha o el peligro que motiva la injerencia alcanza un determinado umbral. El deber del Estado de proteger otros intereses jurídicos está limitado además por la prohibición de injerencias indebidas en los derechos fundamentales. Los umbrales pertinentes para llevar a cabo las medidas que constituyen injerencias deben establecerse en disposiciones legales".

“Cuando la injerencia en los derechos fundamentales es especialmente intrusiva, la medida ya puede ser desproporcionada como tal si los motivos de injerencia expuestos en su fundamento jurídico no tienen suficiente peso. En la medida en que la ley aplicable sirva para evitar determinados peligros, como es el caso aquí según el artículo 1 de la Ley de Protección de la Constitución de Renania del Norte-Westfalia, la importancia y la naturaleza de la amenaza para los intereses protegidos a la que se refiere la disposición respectiva son esenciales para determinar el peso atribuido a los motivos de injerencia.

Si los intereses que la disposición legal que autoriza las injerencias pretende proteger son, como tales, lo suficientemente importantes como para justificar las injerencias en los derechos fundamentales de ese tipo, el principio de proporcionalidad da lugar a otros requisitos constitucionales relativos a la base legal, que establece los requisitos previos para la injerencia. A este respecto, el legislador debe mantener un equilibrio entre el tipo y la gravedad de la lesión de los derechos fundamentales, por un lado, y los requisitos legales para llevar a cabo las medidas que constituyen injerencias, por otro. Los requisitos legales relativos al grado de probabilidad necesario y a la base fáctica del pronóstico deben ser proporcionales al tipo y a la intensidad del menoscabo resultante de los derechos fundamentales. Incluso cuando las amenazas que la injerencia pretende conjurar se refieran a intereses jurídicos de peso excepcional, no puede prescindirse del requisito de probabilidad suficiente. Además, la base legal debe someter cualquier injerencia grave en los derechos fundamentales al requisito de que las suposiciones y conclusiones que motivan la injerencia se basen en hechos concretos”.

“El principio de proporcionalidad pone límites a una disposición legal que autoriza el acceso encubierto a los sistemas informáticos en la medida en que da lugar a requisitos especiales en cuanto a los motivos de la injerencia”.

“Una injerencia de este tipo sólo puede autorizarse si la base legal la supedita a la existencia de indicios fácticos de un peligro concreto para un interés jurídico excepcionalmente significativo. Estos intereses jurídicos excepcionalmente importantes incluyen principalmente la vida, la integridad física y la libertad de la persona. También incluyen los intereses públicos que son de tal importancia que una amenaza para ellos afectaría a los fundamentos o a la existencia del Estado, o a los fundamentos de la existencia humana. Entre ellos se incluye, por ejemplo, el funcionamiento de infraestructuras públicas esenciales y vitales”.

“Para la protección de otros intereses jurídicos, [...] las medidas estatales deben limitarse a las facultades de investigación existentes conferidas con fines de prevención en el respectivo ámbito del Derecho”.

“Como requisito previo para el acceso encubierto, la base legal también debe exigir que existan al menos ciertos indicios fácticos de un peligro específico para los intereses protegidos de suficiente peso establecidos en la disposición pertinente”.

“Dada la exigencia de indicios fácticos, las meras suposiciones o conclusiones extraídas de la experiencia general no bastan por sí solas para justificar el acceso encubierto. Más bien, deben establecerse hechos concretos que apoyen un pronóstico de peligro”.

“Este pronóstico debe apuntar a la existencia de un peligro concreto. Esto significa que debe existir una situación de hecho en la que sea suficientemente probable, en el caso individual, que determinadas personas causen daños a los intereses protegidos por la disposición legal pertinente en un futuro previsible, a menos que el Estado intervenga. La existencia de un peligro concreto viene determinada por tres criterios: se refiere a un caso individual; es previsible que el peligro dé lugar a un daño real en un plazo determinado; y la causa del peligro puede atribuirse a personas

concretas. Sin embargo, el acceso a los sistemas de tecnología de la información en cuestión puede estar justificado ya en un momento en el que no pueda establecerse con suficiente probabilidad que el peligro se materializará en un futuro próximo, siempre que ya existan hechos concretos que indiquen un peligro inminente en el caso individual en relación con un interés jurídico excepcionalmente significativo. En primer lugar, debe ser posible al menos determinar, basándose en estos hechos, el tipo de incidente que podría producirse, y que se producirá en un plazo previsible; en segundo lugar, los hechos deben indicar la implicación de personas concretas cuya identidad se conozca al menos hasta tal punto que las medidas de vigilancia puedan dirigirse a ellas y limitarse en su mayor parte a ellas".

"En cambio, no se tiene suficientemente en cuenta el peso de las injerencias derivadas del acceso encubierto a un sistema informático cuando las disposiciones legales autorizan la medida por motivos de naturaleza tan cautelar que ya no es necesario prever en absoluto la existencia de un peligro concreto para los intereses jurídicos protegidos, ni siquiera en lo que respecta a sus características básicas".

"Por lo que respecta al acceso encubierto a sistemas informáticos, los requisitos constitucionales relativos a los motivos de hecho que dan lugar a la injerencia se aplican a todos los casos en que las disposiciones legales autorizan injerencias en los derechos fundamentales que sirven al objetivo de prevenir peligros. Dado que en todos estos supuestos el perjuicio resultante de la injerencia para las personas afectadas es el mismo, no es necesario establecer requisitos diferentes para las distintas autoridades, por ejemplo, diferenciando entre autoridades policiales y otras autoridades encargadas de tareas preventivas, como las oficinas de protección de la Constitución. A efectos de ponderar el acceso encubierto a los sistemas de tecnología de la información, es en principio irrelevante que la policía y las oficinas para la protección de la Constitución tengan responsabilidades y competencias diferentes y que, en consecuencia, la profundidad de la injerencia resultante de sus medidas pueda diferir".

"Además, las disposiciones legales que autorizan el acceso encubierto a los sistemas informáticos deben prever garantías procesales adecuadas que protejan los intereses de las personas afectadas. En particular, dicho acceso debe estar sujeto, por lo general, a autorización judicial".

"El requisito de autorización judicial permite la revisión previa de una medida de investigación encubierta prevista por una autoridad independiente y neutral, lo que puede contribuir significativamente a la protección efectiva de los derechos fundamentales".

"Si una medida de investigación encubierta supone una injerencia grave en los derechos fundamentales, se requiere constitucionalmente la revisión previa por una autoridad independiente porque, de lo contrario, la persona afectada no gozaría de ninguna protección".

"El legislador sólo puede confiar a una autoridad no judicial el ejercicio de este control si dicha autoridad garantiza el mismo nivel de independencia y neutralidad que un juez. Al pronunciarse sobre la legalidad de la medida encubierta, dicha autoridad de control también está obligada a motivar su decisión".

"Este requisito de revisión previa por una autoridad neutral adecuada puede suprimirse excepcionalmente en casos urgentes, por ejemplo, en casos de peligro que requieran una acción inmediata (*Gefahr im Verzug*); sin embargo, debe garantizarse que en estos casos la autoridad neutral lleve a cabo una revisión a posteriori de la medida. En este contexto, la declaración de urgencia debe cumplir ciertas condiciones de hecho y de derecho informadas por el derecho constitucional".

“Sobre la base de estas normas, la disposición impugnada no cumple los requisitos constitucionales”.

“Según el artículo 5, apartado 2, en relación con el artículo 7, apartado 1, número 1, y el artículo 3, apartado 1, de la Ley de protección de la Constitución de Renania del Norte-Westfalia, el uso de métodos de los servicios de inteligencia por parte de la Oficina del Estado federado para la protección de la Constitución sólo está sujeto a la condición de que existan indicios fácticos que sugieran que estos métodos permiten recabar información sobre actividades inconstitucionales. Ello no somete el ejercicio de estas facultades a un umbral suficientemente sustantivo, ni en cuanto a las condiciones fácticas para llevar a cabo la injerencia, ni en cuanto al peso de los intereses jurídicos que la medida pretende proteger. Además, la disposición no garantiza la revisión previa por parte de una autoridad independiente, por lo que faltan las garantías procesales exigidas por la Constitución”.

“Estas deficiencias no se subsanan, ni siquiera cuando se tiene en cuenta-a pesar de su falta de especificidad jurídica- la referencia legal en el artículo 5(2) número 11 segunda frase de la Ley de protección de la Constitución de Renania del Norte-Westfalia a los requisitos más detallados para las medidas de vigilancia en virtud de la Ley del artículo 10, y cuando se interpreta esta referencia en sentido amplio, como sugiere el Gobierno del Estado federado de Renania del Norte-Westfalia, en el sentido de que hace aplicables todas las garantías formales y sustantivas establecidas en la Ley del artículo 10. Mientras que el artículo 3(1) de la Ley del artículo 10 establece las condiciones para el uso de la vigilancia de las telecomunicaciones, el acceso encubierto a un sistema de tecnología de la información de conformidad con el artículo 5(2) número 11 primera frase, segunda alternativa de la Ley de Protección de la Constitución de Renania del Norte-Westfalia no se limita a la vigilancia de las telecomunicaciones, sino que la disposición permite en general el acceso encubierto para obtener todos los datos disponibles de un sistema de tecnología de la información”.

“Los motivos de injerencia establecidos en el apartado 1 del artículo 3 de la Ley del artículo 10 no satisfacen los requisitos constitucionales, ni en lo que respecta al umbral para el ejercicio de las competencias pertinentes ni en lo que respecta a las garantías procesales”.

“De conformidad con la primera frase del apartado 1 del artículo 3 de la Ley del artículo 10, las medidas de vigilancia son permisibles si existen indicios fácticos que apoyen la sospecha de que alguien está planeando, cometiendo o ha cometido un delito enumerado en el catálogo establecido en dicha disposición. En primer lugar, el catálogo de infracciones penales no parece basarse en un concepto global en virtud del cual todas las infracciones penales enumeradas en dicho catálogo constituyan motivos suficientes que puedan justificar la adopción de medidas con arreglo al artículo 5, apartado 2, número 11, primera frase, segunda alternativa, de la Ley de protección de la Constitución de Renania del Norte-Westfalia. Por lo tanto, no todos los motivos legales previstos en el artículo 10 de la Ley a los que se refiere la disposición impugnada garantizan que el acceso [a sistemas de tecnología de la información] en el caso concreto sirva realmente para proteger uno de los intereses jurídicos excepcionalmente importantes antes mencionados. En segundo lugar, la referencia al artículo 3, apartado 1, primera frase, de la Ley del artículo 10 no garantiza en cada caso que el acceso encubierto a sistemas de tecnología de la información sólo tenga lugar si puede presumirse con suficiente probabilidad que los intereses jurídicos relevantes se pondrán en peligro en un futuro próximo”.

“El artículo 5, apartado 2, número 11, primera frase, segunda alternativa, de la Ley de Protección de la Constitución de Renania del Norte-Westfalia no cumple los requisitos constitucionales relativos a la revisión previa del acceso encubierto a un sistema de tecnología de la información, ni siquiera teniendo en cuenta la referencia al artículo 10 de la Ley”.

“El artículo 10 de la Ley del artículo 10 establece que las medidas de vigilancia deben ser autorizadas mediante una orden emitida por el ministerio competente del Estado federado a petición de la Oficina del Estado federado para la protección de la Constitución. Este procedimiento no es suficiente para garantizar la revisión previa exigida por el artículo 2(1) en relación con el artículo 1(1) de la Ley Fundamental. La disposición anterior no establece ni un requisito de autorización judicial, ni —dado que la revisión previa ejercida por el Comité del artículo 10 (*G 10-Kommission*) según el artículo 3(6) de la Ley sobre la aplicación de la Ley del artículo 10 no está incluida en la referencia legal en cuestión— un mecanismo de supervisión equivalente”.

“Por último, no existen salvaguardias legales adecuadas para garantizar que las medidas adoptadas en virtud del artículo 5, apartado 2, número 11, primera frase, segunda alternativa, de la Ley de Protección de la Constitución de Renania del Norte-Westfalia no interfieran en el núcleo de la vida privada, que goza de protección absoluta”.

“Las medidas de vigilancia encubierta por parte del Estado deben respetar el núcleo inviolable de la vida privada protegido por el artículo 1(1) de la Ley Fundamental. Ni siquiera los intereses públicos superiores pueden justificar una injerencia en este núcleo. El desarrollo de la personalidad dentro del núcleo de la vida privada abarca la posibilidad de expresar procesos internos como emociones y sentimientos, así como reflexiones, opiniones y experiencias de carácter muy personal, sin temor a la vigilancia de las autoridades estatales”.

“En el contexto del acceso encubierto a los sistemas de tecnología de la información, existe el riesgo de que el Estado recopile datos personales que puedan atribuirse al núcleo de la vida privada. Éste es el caso, por ejemplo, cuando la persona en cuestión utiliza el sistema para crear y almacenar archivos con contenidos muy personales, como notas tipo diario o archivos privados de vídeo o sonido. Dichos archivos pueden gozar de protección absoluta, al igual que, entre otros, los relatos escritos de experiencias muy personales. Además, si el sistema también sirve para fines de telecomunicaciones, podría utilizarse para transmitir contenidos que también pueden pertenecer al núcleo de la vida privada. Esto se aplica no sólo a la telefonía vocal, sino también a las comunicaciones a distancia, por ejemplo, a través del correo electrónico u otros servicios de comunicación por Internet”.

“En caso de acceso encubierto a sistemas de tecnología de la información, se requieren garantías legales especiales que protejan el núcleo de la vida privada de la persona afectada”.

“Los ciudadanos utilizan cada vez más sistemas informáticos complejos para la gestión de sus asuntos personales y para las telecomunicaciones, incluso con sus allegados. Estos sistemas les brindan oportunidades de desarrollo en el ámbito altamente personal. En comparación con otras medidas de vigilancia-como el uso del GPS como herramienta de vigilancia técnica-, una medida de investigación que accede a un sistema de tecnología de la información, que puede utilizarse para recopilar datos exhaustivos del sistema objetivo, da lugar así a un mayor riesgo de que se recopilen datos altamente personales”.

“Dado que el acceso se lleva a cabo de forma encubierta, las personas afectadas no tienen la posibilidad de tomar medidas para asegurarse, antes o durante la medida de investigación, de que la autoridad investigadora respeta el núcleo de su vida privada. Esta pérdida total de control debe contrarrestarse con disposiciones especiales que ofrezcan protección mediante garantías procesales adecuadas contra el riesgo de violación del núcleo de la vida privada”.

“Los requisitos constitucionales relativos al diseño específico del marco que garantiza la protección del núcleo pueden diferir en función del método de recogida de datos y de la naturaleza de la información obtenida por el mismo”.

“Una disposición legal que autorice una medida de vigilancia que pueda afectar al núcleo de la vida privada debe garantizar, en la medida de lo posible, que no se recopile ningún dato relacionado con el núcleo de la vida privada. Si es prácticamente inevitable que se obtenga información antes de que pueda determinarse su relación con el núcleo —como ocurre con el acceso encubierto a los sistemas de tecnología de la información—, debe garantizarse una protección suficiente en la fase de análisis. En particular, cuando se hayan encontrado y recopilado datos relativos al núcleo, éstos deberán borrarse sin demora y deberá descartarse cualquier uso posterior”.

“En el contexto del acceso encubierto a un sistema informático, la recogida de datos se automatizará por razones técnicas, al menos en la gran mayoría de los casos. En comparación con la recogida de datos realizada manualmente, este proceso automatizado hace más difícil distinguir en la fase de recogida entre datos relativos al núcleo y datos no relativos al núcleo”.

“Incluso si se accede directamente a los datos de forma manual sin depender de grabaciones técnicas previas, por ejemplo, escuchando la telefonía vocal a través de Internet, la protección del núcleo se enfrenta a dificultades prácticas incluso en la fase de recopilación de datos. Normalmente, cuando se lleva a cabo una medida de vigilancia de este tipo, no puede predecirse con certeza cuál será el contenido de los datos recogidos (en relación con la vigilancia de las telecomunicaciones). También puede resultar difícil analizar el contenido de los datos durante el proceso de recogida. Esto se aplica, por ejemplo, a los archivos de texto o a las conversaciones en lenguas extranjeras. A este respecto, no siempre es posible evaluar, antes o durante la recogida de datos, si las comunicaciones vigiladas pertenecen al núcleo de la vida privada. Sin embargo, si existe el riesgo de que la recogida de datos vulnere el núcleo de la vida privada, esto no significa que el derecho constitucional impida el acceso a dicha información desde el principio en estos casos, dado que el acceso a los sistemas de tecnología de la información se basa en indicios fácticos de un peligro específico para un interés jurídico excepcionalmente significativo”.

“La protección del núcleo, exigida constitucionalmente, puede garantizarse mediante un doble concepto de protección”.

“La disposición legal debe garantizar que la recogida de datos relativos al núcleo se evite desde el principio en la medida en que sea posible en términos de tecnología de la información y técnica de investigación (en relación con la vigilancia de las telecomunicaciones; en relación con la vigilancia acústica de domicilios privados). En particular, deben utilizarse las garantías que ofrecen las tecnologías de la información. Si hay indicios específicos que sugieren que una determinada medida de recogida de datos afectará al núcleo de la vida privada en el caso concreto, en principio no debe utilizarse. La situación es diferente si, por ejemplo, indicios específicos sugieren que los contenidos de comunicación relacionados con el núcleo están deliberadamente vinculados a los contenidos objeto de la investigación con el fin de eludir la vigilancia”.

“En muchos casos, la medida en que los datos recogidos se refieren al núcleo de la vida privada no puede determinarse antes o durante la recogida. El legislador debe prever garantías procesales adecuadas para garantizar que, cuando se recojan datos relativos al núcleo de la vida privada, la gravedad de la violación del núcleo y su impacto en la personalidad y el desarrollo de la persona afectada se reduzcan al mínimo”.

“Deben establecerse procedimientos adecuados que protejan suficientemente los intereses de las personas afectadas. Si el examen revela que se han recogido datos relativos al núcleo de la vida privada, deben suprimirse sin demora. Debe excluirse cualquier intercambio o uso de estos datos”.

“La Ley impugnada carece de las disposiciones necesarias para proteger el núcleo. Incluso si se tuviera en cuenta la referencia a la Ley del artículo 10 en el artículo 5, apartado 2, número 11, segunda frase, de la Ley de protección de la Constitución de Renania del Norte-Westfalia, a pesar de sus deficiencias en términos de especificidad jurídica, ello no merecería una conclusión diferente, dado que la Ley del artículo 10 carece igualmente de salvaguardias que protejan el núcleo de la vida privada”.

“La violación del derecho general de la personalidad en su manifestación como protección de la confidencialidad e integridad de los sistemas de tecnología de la información (art. 2(1) en relación con el art. 1(1) de la Ley Fundamental) anula el artículo 5(2) número 11, primera frase, segunda alternativa, de la Ley de Protección de la Constitución de Renania del Norte-Westfalia. 1(1) de la Ley Fundamental) hace nulo el artículo 5(2) número 11 primera frase, segunda alternativa de la Ley de Protección de la Constitución de Renania del Norte-Westfalia”.

“La autorización legislativa de la vigilancia encubierta de Internet con arreglo al artículo 5, apartado 2, número 11, primera frase, primera alternativa, de la Ley de protección de la Constitución de Renania del Norte-Westfalia viola la intimidad de las telecomunicaciones con arreglo al artículo 10, apartado 1, de la Ley Fundamental. 10(1) de la Ley Fundamental. En determinados casos, las medidas adoptadas en virtud de esta disposición constituyen injerencias en este derecho fundamental que no están justificadas en virtud del derecho constitucional. Artículo 19(1) segunda frase de la Ley Fundamental. Dado que la disposición es inconstitucional, se declara nula. No obstante, la Oficina del Estado para la Protección de la Constitución puede, en principio, llevar a cabo medidas de vigilancia de Internet en la medida en que no equivalgan a injerencias en los derechos fundamentales”.

“La vigilancia encubierta de Internet prevista en el artículo 5, apartado 2, número 11, primera frase, primera alternativa, de la Ley de protección de la Constitución de Renania del Norte-Westfalia abarca las medidas llevadas a cabo por la Oficina de Protección de la Constitución para obtener conocimiento del contenido de las comunicaciones por Internet a través de los medios técnicos normales previstos a tal fin, por ejemplo, accediendo a un sitio web en la World Wide Web mediante un navegador web (véase el artículo A I 1 a supra). La disposición impugnada no justifica tal injerencia en virtud del Derecho constitucional”.

“El ámbito de protección del artículo 10(1) de la Ley Fundamental cubre las telecomunicaciones en curso realizadas a través de un sistema de tecnología de la información conectado a Internet. Sin embargo, este derecho fundamental sólo protege a los individuos en la medida en que tengan la expectativa legítima de que terceros no puedan tener conocimiento de las telecomunicaciones en las que participan. Por el contrario, esta protección de los derechos fundamentales no se extiende a las expectativas legítimas que los interlocutores de las telecomunicaciones tienen entre sí. Por lo tanto, el hecho de que el Estado obtenga conocimiento de los contenidos de las telecomunicaciones sólo debe medirse contra la intimidad de las telecomunicaciones si una autoridad estatal vigila una relación de telecomunicaciones desde el exterior sin estar implicada como parte comunicante”.

“Por lo tanto, la vigilancia encubierta de Internet interfiere con el artículo 10(1) de la Ley Fundamental si la Oficina de Protección de la Constitución vigila el contenido de comunicaciones seguras utilizando claves de acceso obtenidas sin el consentimiento o contra la voluntad de las

partes comunicantes. Este es el caso, por ejemplo, si se utiliza una contraseña obtenida mediante *keylogging* para acceder a la bandeja de entrada de un correo electrónico o a un chat privado".

"Por el contrario, no hay interferencia con el artículo 10(1) de la Ley Fundamental si, por ejemplo, un participante en un chat privado ha facilitado voluntariamente a una persona que actúa en nombre de la Oficina de Protección de la Constitución su información de acceso, que la autoridad utiliza a continuación. Una injerencia en la intimidad de las telecomunicaciones puede descartarse ciertamente cuando la autoridad recopila contenidos de acceso general, por ejemplo, mediante la inspección de foros de debate abiertos o sitios web que no están protegidos por contraseña".

"Las injerencias en el artículo 10(1) de la Ley Fundamental derivadas del artículo 5(2) número11 primera frase, primera alternativa de la Ley de Protección de la Constitución de Renania del Norte-Westfalia no están justificadas con arreglo al derecho constitucional. La disposición impugnada no cumple los requisitos constitucionales relativos a las autorizaciones para tales injerencias".

"El artículo 5, apartado 2, número 11, primera frase, primera alternativa, de la Ley de Protección de la Constitución de Renania del Norte-Westfalia no cumple el requisito de claridad y especificidad jurídicas, dado que la segunda frase de esta disposición es demasiado vaga y no establece los requisitos previos para la injerencia de manera suficientemente precisa".

"Además, en la medida en que se compara con el artículo 10.1 de la Ley Fundamental, la disposición impugnada no cumple el requisito de proporcionalidad en sentido estricto".

"La injerencia en la intimidad de las telecomunicaciones es grave. Basándose en la disposición impugnada, la Oficina de Protección de la Constitución podría acceder a contenidos de comunicaciones que pueden ser sensibles y que pueden proporcionar información sobre asuntos personales y hábitos de las personas afectadas. Esto es válido no sólo para las personas que provocaron una medida de vigilancia; la interferencia también puede afectar indiscriminadamente a otras personas si la información obtenida se refiere no sólo a las personas objeto de la medida, sino también a sus interlocutores. El carácter encubierto del acceso aumenta la gravedad de la injerencia. Además, dada la amplia redacción de los requisitos previos para la injerencia en el artículo 7(1) número1 en relación con el artículo 3(1) de la Ley de protección de la Constitución de Renania del Norte-Westfalia, la vigilancia también puede dirigirse contra personas que no hayan provocado la injerencia".

"Incluso teniendo en cuenta el peso significativo que se concede al objetivo perseguido de proteger el orden constitucional, una injerencia en los derechos fundamentales de tal gravedad requiere en principio al menos que la base jurídica establezca un umbral cualificado y sustantivo para la injerencia (en relación con las investigaciones penales). A falta de dicho umbral, el artículo 7, apartado 1, número 1, en relación con el artículo 3, apartado 1, de la Ley de protección de la Constitución de Renania del Norte-Westfalia autoriza, a gran escala, una acción puramente cautelar del servicio de inteligencia antes de que se materialicen peligros concretos, pero no tiene en cuenta el peso de los intereses jurídicos, incluidos los de terceros, que pueden verse vulnerados como consecuencia de ello. Una autorización legislativa tan amplia de injerencias en los derechos fundamentales no es compatible con el principio de proporcionalidad".

"Con respecto a las injerencias derivadas del artículo 5, apartado 2, número 11, primera frase, primera alternativa, de la Ley de protección de la Constitución de Renania del Norte-Westfalia, el marco legal no contiene ninguna salvaguardia que proteja el núcleo de la vida privada. Sin embargo, tales salvaguardias son necesarias en todos los casos en que las autoridades estatales están autorizadas a recopilar contenidos de telecomunicaciones de una manera que interfiere con el artículo 10(1) de la Ley Fundamental".

“Por último, en la medida en que el artículo 5, apartado 2, número11, primera frase, primera alternativa, de la Ley de protección constitucional de Renania del Norte-Westfalia autoriza injerencias en el artículo 10, apartado 1, de la Ley Fundamental, la disposición no cumple el requisito de que el derecho fundamental afectado esté expresamente especificado (*Zitiergebot*) de conformidad con el artículo 19, apartado 1, segunda frase, de la Ley Fundamental. 10(1) de la Ley Fundamental, la disposición no cumple el requisito de que el derecho fundamental afectado esté expresamente especificado (*Zitiergebot*) de conformidad con el artículo 19(1) segunda frase de la Ley Fundamental”.

“Dado que el artículo 5(2) número11 primera frase, primera alternativa de la Ley de Protección de la Constitución de Renania del Norte-Westfalia viola el artículo 10(1) y artículo 19(1) segunda frase de la Ley Fundamental, la disposición es nula”.

“Sin embargo, en la medida en que las medidas de vigilancia de Internet no interfieran con los derechos fundamentales, la nulidad de la autorización legislativa no impide en general que la autoridad adopte tales medidas”.

“La vigilancia encubierta que no suponga una injerencia en el artículo 10(1) de la Ley Fundamental no constituye necesariamente una injerencia en el derecho general a la personalidad garantizado por el artículo 2(1) en relación con el artículo 1(1) de la Ley Fundamental”.

“La confidencialidad y la integridad de los sistemas de tecnología de la información garantizados por el derecho general de la personalidad no se ven afectados por las medidas de vigilancia de Internet con arreglo al artículo 5, apartado 2, número 11, primera frase, primera alternativa, de la Ley de protección de la Constitución de Renania del Norte-Westfalia, dado que estas medidas se limitan a recopilar datos destinados por el propietario del sistema en cuestión-por ejemplo, el operador de un servidor web- para fines de comunicación por Internet utilizando los medios técnicos normales previstos a este respecto. Por lo tanto, no pueden esperar legítimamente que se tomen tales medidas”.

“Por regla general, tampoco hay interferencia con el artículo 2(1) en relación con el artículo 1(1) de la Ley Fundamental en su manifestación como derecho a la autodeterminación informativa”.

“En general, no se prohíbe al Estado obtener información de acceso público, lo que también se aplica si esta posibilidad se utiliza para recopilar información personal en el caso concreto [...]. Por lo tanto, no supone una injerencia en el derecho general de la personalidad el hecho de que una autoridad estatal recopile contenidos de comunicación disponibles en Internet y dirigidos al público en general o a un grupo de personas que no está definido con mayor precisión. Este es el caso, por ejemplo, cuando las autoridades consultan un sitio web de acceso general en la World Wide Web, se suscriben a una lista de correo abierta a todo el mundo o supervisan una sala de chat abierta”.

“Sin embargo, puede producirse una injerencia en el derecho a la autodeterminación informativa si la información obtenida mediante la visualización de contenidos web de acceso general se recopila, almacena y, en su caso, analiza deliberadamente utilizando otros datos, lo que da lugar a un riesgo especial para la personalidad de la persona afectada. Tales medidas requieren una base legal que autorice esta interferencia”.

“No constituye una injerencia en el derecho a la autodeterminación informativa el mero hecho de que una autoridad estatal utilice una identidad encubierta para entablar una relación de comunicación con un titular de derechos fundamentales. Sin embargo, sí constituye una injerencia si, al hacerlo, se aprovecha de las expectativas legítimas de esa persona en relación con

la identidad y la motivación de su interlocutor, con el fin de recopilar datos personales que la autoridad estatal no recibiría de otro modo [...]".

"De ello se deduce que, por regla general, la vigilancia de Internet como tal no constituye una injerencia en los derechos fundamentales. En gran medida, las relaciones de comunicación facilitadas por los servicios de comunicación por Internet no merecen expectativas legítimas en cuanto a la identidad y autenticidad de los interlocutores, ya que no pueden verificarse. Esto se aplica incluso si ciertas personas —por ejemplo, en el contexto de un foro de debate— participan en la comunicación durante un período de tiempo más largo y forman así una especie de ´comunidad en línea´. Incluso en este tipo de relaciones de comunicación, todos los participantes son conscientes de que no conocen la identidad de sus interlocutores o, en cualquier caso, no pueden verificar la información que éstos proporcionan sobre sí mismos. Por lo tanto, su expectativa de que no se están comunicando con una autoridad estatal no merece protección".

"El artículo 5a(1) de la Ley de protección de la Constitución de Renania del Norte-Westfalia es compatible con la Ley Fundamental en la medida en que su ámbito de aplicación se ha ampliado para abarcar actividades en el sentido del artículo 3(1) número 1 de la Ley de protección de la Constitución de Renania del Norte-Westfalia. En particular, esta disposición no viola el art. 2(1) en relación con el artículo 1(1) de la Ley Fundamental. La recogida de datos sobre cuentas y transacciones bancarias prevista en el artículo 5a(1)de la Ley de Protección de la Constitución de Renania del Norte-Westfalia interfiere con el derecho general de la personalidad en su manifestación como derecho a la autodeterminación informativa. [...]. Las injerencias en los derechos fundamentales autorizadas por el artículo 5a(1) de la Ley de Protección de la Constitución de Renania del Norte-Westfalia están, sin embargo, constitucionalmente justificadas con respecto a la investigación de las actividades especificadas en el artículo 3(1) número1 de la Ley de Protección de la Constitución de Renania del Norte-Westfalia".

5. LÍMITES EN LA BÚSQUEDA DE INFORMACIÓN EN PERICIAS INFORMÁTICAS Y PROTECCIÓN DE DATOS PERSONALES

JURISPRUDENCIA NACIONAL

5.1. JUZGADO DE 1RA INSTANCIA EN LO PENAL CONTRAVENCIONAL Y DE FALTAS N° 5, SECRETARÍA N°9. "REQUENA MORA Y OTROS". CAUSA N°204761/2021. REGISTRO N° 2047924/2021. 28/9/2021.

HECHOS

A raíz de una causa penal por falsificación de instrumento público, la fiscalía solicitó al juez de garantías una pericia al teléfono celular de la persona sospechada sin especificar qué aplicaciones o un rango de fechas determinado.

DECISIÓN

El Juzgado de Primera Instancia en lo Penal, Contravencional y de Falta N°5 de la Ciudad Autónoma de Buenos Aires no hizo lugar al pedido del fiscal (jueza Botana).

ARGUMENTOS

1. Telefonía celular. Derecho a la intimidad. Derecho a la privacidad. Protección de datos personales.

"[E]n la actualidad los aparatos celulares recaudan abundante cantidad de información sensible y de carácter estrictamente personal, que, como tal, se encuentra constitucionalmente resguardada de intromisiones e injerencias injustificadas —conforme los artículos 12 de la Constitución de la CABA y 18 y 19 Constitución Nacional—.

"[P]ara autorizar la apertura e inspección de un teléfono celular, irremediablemente se requiere que *ex ante* se encuentren acreditados elementos objetivos y circunstancias de urgencia que lo justifiquen, y, en esos casos, la medida debe estar debidamente delimitada".

"No se advierte la existencia de ningún indicio ni elemento objetivo que —al menos en este momento incipiente de la investigación— permita conectar la simple conducta del uso o la exhibición de una licencia de conducir apócrifa en la vía pública con la información que podría estar contenida en su teléfono celular".

La fiscalía reiteró un nuevo pedido de inspección al teléfono celular con circunscripción de las plataformas y lapso temporal. La jueza lo rechazó y el representante del Ministerio Público apeló esa decisión. La Sala I en lo Penal, Penal Juvenil, Contravencional y de Faltas, revocó lo decisión (jueces Sáez Capel y Vázquez y jueza Marum) y autorizó el análisis del teléfono celular. Consideró que la pericia tenía una vinculación directa con los hechos

5.2. CÁMARA DE APELACIONES EN LO PENAL, CONTRAVENCIONAL Y DE FALTAS, SALA I. "VILLALBA CUYARI". CAUSA N° 11412/2021. REGISTRO N° 2205841/2021. 12/10/2021.

HECHOS

Una persona estaba siendo investigada por la presunta comisión de un delito. En el marco de ese proceso, la fiscalía solicitó la intervención del personal del Cuerpo de Investigaciones Judiciales del Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires para que realizara la pericia informática del teléfono celular de la persona. El juzgado interviniente hizo lugar al pedido de la fiscalía y autorizó la pericia del dispositivo móvil para que se determine la existencia de programas o aplicaciones de mensajería que pudieran contener información sobre la compra, venta, tenencia, distribución, facilitación y/o comercialización de estupefacientes y para que se analice la agenda de contactos del dispositivo con el objeto de determinar posibles compradores. Contra esa decisión, la defensa interpuso un recurso de apelación. Para ello, sostuvo que la requisa lesionaba el ámbito de privacidad e intimidad de la persona ya que la medida era irrazonable pues no existía una proporción entre el fin perseguido y los medios utilizados y porque la medida carecía de una delimitación temporal de la información que se buscaba.

DECISIÓN

La Sala I de la Cámara de Apelaciones en lo Penal, Contravencional y de Faltas de la Ciudad Autónoma de Buenos Aires, por unanimidad, confirmó la resolución que autorizaba la requisa, pero dispuso que se dicte un nuevo pronunciamiento y se establezca la delimitación temporal del objeto de la medida.

ARGUMENTOS

1. **Control de Constitucionalidad. Telefonía celular. Prueba. Prueba informática. Orden judicial. Derecho a la intimidad. Plazo.**

"[E]n el presente caso se cuestiona la pericia ordenada sobre el teléfono celular, es importante dejar asentado que el derecho a la intimidad está constitucionalmente consagrado, en los artículos 18 y 19 de nuestra Carta Magna, y en el artículo 13.8 de la Constitución de la Ciudad, y que ello implica que las intromisiones en ese ámbito, tales como los allanamientos de domicilio; las escuchas telefónicas, del secuestro de papeles y correspondencia o información personal almacenada, sólo pueden ser ordenadas por el juez competente".

"[N]o se puede soslayar el hecho de que una pericia, en este caso, sobre el teléfono celular del encausado, no solamente está en pugna con el derecho [a la intimidad], sino que, a su vez, implica también la producción de prueba de cargo anticipada, esto es, previa a la etapa de debate oral, que es el escenario constitucionalmente establecido para ese fin".

"[L]a pericia en cuestión constituye una excepción permitida a la regla [que establece que la prueba debe producirse en la etapa de debate], en la medida en que se trata de una prueba irrepetible y que debe ser llevada a cabo en esta etapa primigenia de la investigación, para orientar su curso".

"[U]na medida como la ordenada constituye una injerencia sobre derechos reconocidos constitucionalmente, cuya transgresión posee una interpretación restrictiva, y que configura, al mismo tiempo, una ´prueba anticipada´, debe tener una concreta intervención jurisdiccional, a fin de poder garantir, precisamente, el derecho de defensa".

“[E]s necesario establecer una delimitación de su objeto y su alcance, para con ello otorgar una posibilidad material de control, que no se constituya en una mera invocación formal”.

“[E]n el caso, se indicaron cuáles eran los motivos por los que la pericia era necesaria, se la circunscribió a la información que pudiera encontrarse en el dispositivo y relativa a los puntos que fueron detallados para el examen [...]”.

“[L]a medida no excede el marco de la investigación, en los términos en que se delimitó. Todo ello garantiza que se obtenga sólo esa información y que no se registren otros datos que no sean los buscados”.

“[L]a Juez indicó que la medida solicitada deberá realizarse con la debida intervención de las partes y seguir las prescripciones previstas por los artículos 139 y sgtes del CPPCABA, por lo que debe llevarse a cabo en presencia de la defensa y estará a cargo de personal especializado. Ello descarta que la falta de precisión del software que se va a utilizar para extraer los datos genere algún agravio de magnitud tal que amerite ser considerado a los fines de impedir su realización”.

“[T]al como lo sostuvo la defensa, no se estableció período de tiempo determinado. En virtud de ello, resulta palmaria la diferencia entre este caso concreto y otros precedentes de esta Sala en la materia, en los que el Juez de grado había realizado una correcta delimitación de la medida autorizada”.

“[S]i bien la *a quo* ha analizado la solicitud de la Fiscalía con la rigurosidad que una medida de esta clase impone, acierta la defensa cuando menciona que carece de determinación temporal, lo cual implica un desacierto. En el caso, ese mandato de limitación y regulación no fue cumplimentado ni por la fiscalía en oportunidad de solicitar la autorización para realizar la pericia, ni por la jueza de grado, en la medida en que de su resolución no se desprende el lapso temporal que corresponde establecer y que delimita su alcance”.

“[C]orresponde autorizar el análisis del teléfono celular, oportunamente secuestrado. Sin embargo, de forma previa a ello, la magistrada de grado deberá especificar el alcance de dicha medida estableciendo la delimitación temporal de su objeto de estudio”.

5.3. CÁMARA DE APELACIONES EN LO PENAL, PENAL JUVENIL, CONTRAVENCIONAL Y DE FALTAS, SALA I. "REQUENA MORA Y OTROS". CAUSA N° 204761/2021. REGISTRO N° 698479/2022. 4/4/2022.

HECHOS

A raíz de una causa penal por falsificación de instrumento público, la fiscalía solicitó al juez de garantías una pericia al teléfono celular de la persona investigada sin especificar un rango de fechas determinado ni tampoco qué aplicaciones serían analizadas. El Juzgado de Primera Instancia en lo Penal, Contravencional y de Falta N°5 no hizo lugar al pedido del fiscal. La fiscalía reiteró un nuevo pedido de inspección al teléfono celular con circunscripción de las aplicaciones y del lapso temporal. La jueza lo rechazó y el representante del Ministerio Público apeló esa resolución.

DECISIÓN

La Sala I en lo Penal, Penal Juvenil, Contravencional y de Faltas, revocó la decisión y autorizó el peritaje del teléfono celular pero circunscrito al período comprendido entre el 13/12/2019 y el 13/5/2020 (jueces Sáez Capel y Vázquez y jueza Marum).

ARGUMENTOS

1. Telefonía celular. Prueba. Prueba digital. Prueba informática.

"[A] partir de lo analizado, resulta claro que la solicitud de la pericia fue fundamentada y se explicaron cuáles eran los motivos por los que su realización era necesaria como también se circunscribió la información que pudiera encontrarse en el dispositivo y relativa a los puntos que fueron detallados para el examen [...]".

"[E]ntendemos que, a diferencia de lo sostenido por la magistrada de grado, la medida no excede el marco de la investigación y tiene una vinculación directa con el objeto de la pesquisa, en los términos en que se delimitó".

"A la par que cabe señalar que la medida solicitada debe realizarse con la debida intervención de las partes y seguir las prescripciones previstas por los arts. 139 y sgtes. del CPPCABA, por lo que debe llevarse a cabo en presencia de la defensa, a efectos de su control y evitar algún agravio de magnitud tal que amerite ser considerado a los fines de impedir su realización".

"[D]ado que la pericia fue solicitada con fundamento en el objeto procesal de la investigación resulta ser proporcional con aquello que se pretende desentrañar y se vincula directamente con un elemento secuestrado durante el procedimiento de prevención y detención, en un contexto de flagrancia".

2. Prueba digital. Principio de proporcionalidad. Razonabilidad.

"[L]a medida solicitada [por el fiscal] importa, por su extensión en el tiempo, injustificada y desproporcionada.

"[C]abe añadir que las facultades de investigación del Ministerio Público Fiscal no pueden, en ningún caso, avasallar los derechos constitucionales de los encartados, y que esa prohibición adquiere particular relevancia en aquellas circunstancias en las que [...] las medidas de prueba en

cuestión tienen como norte la identificación de otros individuos que podrían haber participado en el supuesto hecho delictivo".

"[L]a excesiva amplitud en el tiempo de la pericia peticionada en autos no cumple con los principios de idoneidad, necesariedad y proporcionalidad, y que resulta a todas luces excesiva…".

"[E]ntendemos que corresponde autorizar el análisis del teléfono celular [...] medida ésta que deberá circunscribirse al período comprendido entre el 13/12/2019 (esto es, tres meses antes de la fecha en que figura expedida la licencia), hasta el 13/5/2020 —seis meses—, lapso que se evidencia razonable teniendo en cuenta los fines del proceso y los principios de idoneidad, necesariedad y proporcionalidad".

JURISPRUDENCIA INTERNACIONAL

5.4. TRIBUNAL EUROPEO DE DERECHOS HUMANOS, "TRAJKOVSKI Y CHIPOVSKI V. MACEDONIA DEL NORTE". CASOS N° 53205/13 y 63320/13. 13/06/2020.

HECHOS

En febrero y octubre de 2010dos personas fueron detenidas por la policía en Skopje, Macedonia del Norte, bajo sospecha de haber participado en un robo agravado. Debido a las detenciones, se les tomaron muestras de ADN mediante hisopados bucales sin proporcionarles explicación alguna sobre el procedimiento o su finalidad. Posteriormente, ambas personas fueron procesadas y condenadas en suspenso por el delito de robo agravado. En uno de los casos, el análisis de ADN no fue utilizado como evidencia durante el proceso. Las defensas de ambas personas presentaron reclamos individuales ante la Dirección de Protección de Datos Personales de Macedonia del Norte. En sus reclamos señalaron que la toma y retención de sus muestras de ADN constituían una violación de su derecho a la privacidad. Sin embargo, la Dirección desestimó sus quejas. Para ello, la Dirección argumentó que la policía estaba legalmente autorizada a recolectar y procesar datos personales, incluso material genético, con el fin de prevenir y detectar delitos. Contra esa decisión, ambas personas apelaron la medida ante el Tribunal Administrativo y, posteriormente, ante el Tribunal Administrativo Superior. Sin embargo, ambas instancias confirmaron las decisiones anteriores. Sostuvieron que la policía había actuado de acuerdo con la ley al tomar y procesar el material de ADN de personas sospechosas de cometer un delito.

Entonces, luego de agotar todas las vías de recurso internos, ambas personas presentaron distintas solicitudes ante el Tribunal Europeo de Derechos Humanos en agosto y octubre de 2013. En sus demandas, sostuvieron que la normativa interna que permitió a las autoridades la recolección, procesamiento y almacenamiento de su material de ADN violaba el derecho al respeto de la vida privada y familiar. En tal sentido, señalaron que los propósitos para los cuales se podían tomar muestras de ADN y almacenar perfiles estaban formulados en términos demasiado amplios. Además, indicaron que la normativa interna no indicaba la duración de la retención del material de ADN con respecto a las personas condenadas, como era su caso. Por su parte, el Gobierno de Macedonia del Norte defendió sus acciones. Para ello, sostuvo que la interferencia con la vida privada de los solicitantes había sido de acuerdo con la ley, perseguía un objetivo legítimo de detección y prevención del crimen y, además, que era proporcional al objetivo buscado. Asimismo, el Gobierno argumentó que los perfiles de ADN debían ser registrados en los registros relevantes y "retenidos por cierto período de tiempo, pero no indefinidamente". Finalmente, el Gobierno señaló que tales datos "pueden ser retenidos hasta que hayan cumplido el propósito para el cual fueron tomados".

DECISIÓN

El Tribunal Europeo de Derechos Humanos consideró que Macedonia del Norte era responsable por la violación del derecho al respeto de la vida privada (artículo 8 del Convenio Europeo de Derechos Humanos).

ARGUMENTOS

1. Derecho a la vida privada y familiar. Protección de datos personales. Datos biométricos. Derechos Humanos.

"El Tribunal observa que no es discutido por el Gobierno que el material de ADN es información personal y que en los presentes casos hubo una interferencia con el derecho de los solicitantes al respeto de su vida privada. El Tribunal, teniendo en cuenta su jurisprudencia, según la cual los perfiles de ADN constituyen claramente datos relativos a la 'vida privada' de una persona y su retención constituye una interferencia con el derecho al respeto de la vida privada, en el sentido del artículo 8 apartado 1 del Convenio (véase *S. y Marper v. el Reino Unido*), no encuentra razón para sostener lo contrario" (párrafo 43).

"[Se] examinará si la interferencia estaba justificada en términos del artículo 8 apartado 2 del Convenio, es decir, si estaba de acuerdo con la ley, perseguía un objetivo legítimo y era 'necesaria en una sociedad democrática'" (párrafo 44).

"El Tribunal reconoce la importancia de tal información en la detección del crimen y particularmente en el combate de la reincidencia (véase, mutatis mutandis, Gardel v. Francia). Sin embargo, reitera que la mera retención y almacenamiento de datos personales por autoridades debe ser considerado como teniendo un impacto directo en el interés de la vida privada del individuo concernido, independientemente de si se hace un uso posterior de los datos (véase *S. y Marper*)" (párrafo 51).

2. Principio de legalidad. Reglamentación de los derechos. Control de legalidad.

"[Se] observa que la recolección y almacenamiento de material de ADN con respecto a los solicitantes tenía una base en la ley doméstica. De hecho, las disposiciones relevantes de la Ley de Protección de Datos Personales, la Ley de Policía y las Reglas de Conducta Policial, que estaban en vigor al momento en que se tomaron las muestras de ADN de los solicitantes y en las que las autoridades se basaron en sus casos, autorizaban a la policía a recolectar, procesar y almacenar datos personales, incluyendo material de ADN, con el fin de establecer la identidad de una persona que es sospechosa de cometer un crimen" (párrafo 46).

"La existencia de disposiciones legales para la toma y almacenamiento de material de ADN no fue impugnada por los solicitantes. Sin embargo, sostuvieron que ese marco carecía de la calidad requerida en el sentido del artículo 8 del Convenio. En particular, presentaron que los propósitos para los cuales se podían tomar muestras de ADN y almacenar perfiles estaban formulados en términos amplios y que las disposiciones nacionales relevantes no especificaban la duración de la retención del material de ADN con respecto a las personas condenadas, como ellos mismos" (párrafo 47).

"El Tribunal observa que el marco regulatorio sobre la retención de material de ADN no era muy preciso. Sin embargo, las cuestiones relacionadas con las condiciones adjuntas y los arreglos para el almacenamiento de material de ADN están estrechamente relacionadas con la cuestión más amplia de si la interferencia era necesaria en una sociedad democrática" (párrafo 48).

3. Razonabilidad. Principio de proporcionalidad. Política criminal. Control judicial. Democracia.

"El Tribunal está de acuerdo con el Gobierno en que la retención de información de ADN persigue el objetivo legítimo de la detección y, por lo tanto, prevención del crimen. Mientras que la toma original de esta información persigue el objetivo de vincular a una persona particular con el crimen particular del que se sospecha, su retención persigue el propósito más amplio de ayudar en la futura identificación de delincuentes" (párrafo 49).

"Los principios relevantes del Convenio se resumen en la sentencia del Tribunal en el caso de *S. y Marper.* A diferencia de ese caso, que se refería a la retención de datos personales de personas no condenadas, la cuestión en el presente caso es si la retención de los datos de ADN de los

solicitantes, como personas que fueron condenadas por robo agravado, estaba justificada según el artículo 8 apartado 2 del Convenio" (párrafo 50).

"[Se] observa que la legislación aplicable en el momento no establecía un límite de tiempo específico para la retención de datos de ADN de los solicitantes como personas condenadas. De hecho, como declaró el Gobierno, los perfiles de ADN debían ser registrados en los registros relevantes y 'retenidos por cierto [período de] tiempo, pero no indefinidamente'. Que tales datos 'pueden ser retenidos hasta que hayan cumplido el propósito para el cual fueron tomados' está abierto a varias interpretaciones" (párrafo 52).

"[N]o se ha argumentado que la naturaleza o gravedad del delito por el cual una persona fue condenada, o recibió una pena, o cualquier otro criterio definido, como arrestos previos, y cualquier otra circunstancia especial, tenga alguna influencia en la recolección, almacenamiento y retención de registros de ADN (véase, *S. y Marper* y *Peruzzo y Martens v. Alemania*). Además, mientras que la policía está investida con el poder de eliminar datos personales de los registros, la ley guarda silencio sobre las condiciones bajo las cuales se puede hacer y el procedimiento a seguir. Mientras que la ley prevé, en términos generales, la posibilidad de revisión judicial junto con una revisión administrativa previa, no hay disposición que permita una revisión específica de la necesidad de retención de datos. Del mismo modo no hay disposición bajo la cual una persona concernida pueda solicitar que se eliminen los datos que le conciernen si conservar los datos ya no parece necesario en vista de la naturaleza del delito, la edad de la persona concernida, el tiempo transcurrido y la personalidad actual de la persona (véase [caso] *Gardel*)" (párrafo 53).

"[E]l Tribunal considera que la naturaleza general e indiscriminada de las facultades de retención de los perfiles de ADN de los solicitantes, como personas condenadas por un delito, junto con la ausencia de salvaguardias suficientes disponibles para los solicitantes, no logra alcanzar un equilibrio justo entre los intereses públicos y privados en competencia y que el Estado demandado ha sobrepasado el margen de apreciación aceptable a este respecto. Por consiguiente, la retención controvertida constituye una injerencia desproporcionada en el derecho al respeto de la vida privada de los demandantes y no puede considerarse necesaria en una sociedad democrática" (párrafo 54).

5.5. TRIBUNAL EUROPEO DE DERECHOS HUMANOS, "GAUGHRAN V. EL REINO UNIDO". CASO N° 45245/15. 13/06/2020.

HECHOS

En octubre de 2008, una persona fue detenida en un control policial en Newry, Irlanda del Norte, por conducir bajo los efectos del alcohol. Como consecuencia de su arresto, se le tomaron muestras de ADN, huellas dactilares y una fotografía. Posteriormente, en noviembre de 2008, la persona se declaró culpable ante el Tribunal de Magistrados de Newry y, en consecuencia, fue multado y se le prohibió conducir durante 12 meses. Luego, en enero de 2009, su abogado solicitó al Servicio de Policía de Irlanda del Norte (PSNI) la destrucción o devolución de los datos biométricos retenidos. Sin embargo, el PSNI respondió negativamente. Frente a este rechazo, la defensa decidió iniciar un proceso judicial con el objetivo de obtener una revisión judicial de la decisión del PSNI de retener indefinidamente sus datos biométricos. Sin embargo, en noviembre de 2012, el Tribunal Superior de Justicia de Irlanda del Norte desestimó la solicitud. Esta decisión fue apelada ante la Corte Suprema del Reino Unido, la cual, en mayo de 2015, también desestimó su pedido y confirmó lo resuelto por el juzgado de la instancia anterior. Ante este rechazo, y luego de agotarlas vías internas, la persona realizó una petición ante el Tribunal Europeo de Derechos Humanos. En tal sentido, sostuvo que la retención indefinida de su perfil de ADN, huellas dactilares y fotografía, conforme a la política de retención de datos personales de cualquier individuo condenado por un delito registrable, constituía una interferencia desproporcionada con su derecho al respeto de su vida privada y familiar. Además, señaló que esta retención indefinida violaba su derecho a la privacidad, toda vez que no existían salvaguardias adecuadas ni mecanismos de revisión efectivos. Por último, sostuvo que la retención no tomaba en consideración la gravedad del delito cometido ni la necesidad continua de retener los datos. Por su parte, el Gobierno del Reino Unido defendió la legalidad y proporcionalidad de la retención de datos. Para ello, señaló que existía un amplio margen de apreciación en esta materia y que la retención de datos biométricos era valiosa para combatir el crimen. Finalmente, como respaldo a su posición, el Gobierno señaló que varios otros países europeos tenían políticas similares de retención de datos.

DECISIÓN

El Tribunal Europeo de Derechos Humanos consideró que el Reino Unido era responsable por la violación del derecho al respeto de la vida privada y la correspondencia (artículo 8 del Convenio Europeo de Derechos Humanos).

ARGUMENTOS

1. Derecho a la vida privada y familiar. Derecho a la privacidad. Datos biométricos. Protección de datos personales. Sistema de Reconocimiento Facial. Identificación de personas. Vigilancia electrónica.

"El Tribunal observa que el Gobierno no discute que el material de ADN es información personal y que en los presentes casos hubo una interferencia con el derecho del solicitante al respeto de su vida privada. El Tribunal, teniendo en cuenta su jurisprudencia, según la cual los perfiles de ADN constituyen claramente datos relativos a la 'vida privada' de una persona y su retención constituye una interferencia con el derecho al respeto de la vida privada en el sentido del artículo 8 apartado 1 del Convenio (véase *S. y Marper*), no encuentra razón para sostener lo contrario. El Tribunal también ha encontrado previamente que la retención de huellas dactilares constituye una interferencia con el derecho al respeto de la vida privada, en el sentido del artículo 8 apartado

1 del Convenio (véase *S. y Marper*). Por lo tanto, la retención del perfil de ADN y las huellas dactilares del solicitante constituía una interferencia con su vida privada" (párrafo 63).

"El Gobierno también aceptó que la retención de la fotografía del solicitante constituía una interferencia con su vida privada. Al hacerlo, se basó en parte en las conclusiones del Tribunal Superior en RMC. El Tribunal observa que en ninguna etapa de los procedimientos internos se expresó una duda real sobre la conclusión de que la retención de la fotografía del solicitante constituía una interferencia" (párrafo 64).

"Aunque esa cuestión parece haberse resuelto en la jurisprudencia nacional y entre las partes, sigue siendo algo novedosa desde la perspectiva de la jurisprudencia del Tribunal. El Tribunal recuerda que la Comisión previamente encontró que la retención y el uso de fotografías tomadas en el arresto por las autoridades policiales no constituían una interferencia con el derecho al respeto de la vida privada en el sentido del artículo 8 apartado 1 (véase *X v. el Reino Unido*; *Lupker v. los Países Bajo, Kinnunen v. Finlandi*; y *Friedl v. Austria*)" (párrafo 65).

"El caso de *S. y Marper*, no se refería a la retención de fotografías, pero en su sentencia la Gran Sala revisó la jurisprudencia expuesta anteriormente y observó que el concepto de vida privada incluía elementos relacionados con el derecho de una persona a su imagen. En el párrafo siguiente, encontró que al determinar si la información personal retenida por las autoridades involucra alguno de los aspectos de la vida privada mencionados anteriormente, el Tribunal tendrá debidamente en cuenta el contexto específico en el que se ha registrado y retenido la información en cuestión, la naturaleza de los registros, la forma en que se utilizan y procesan estos registros y los resultados que se pueden obtener (véase *S. y Marper*)" (párrafo 66).

"[E]l Tribunal observa que la fotografía del solicitante fue tomada en su arresto para ser almacenada indefinidamente en la base de datos policial local. En el momento de su sentencia en 2014, el Tribunal Supremo encontró que la fotografía de custodia del solicitante se mantenía en una base de datos independiente, limitada al personal policial autorizado y que no tenía la capacidad de comparar fotografías ya sea por reconocimiento facial o de otra manera" (párrafo 67).

"[T]ras la sentencia del Tribunal Superior en RMC, el Ministerio del Interior produjo un informe para Inglaterra y Gales (la Revisión del Ministerio del Interior sobre el Uso y Retención de Imágenes de Custodia) que esbozó con cierto detalle el funcionamiento de las bases de datos relevantes y el uso de tecnología de reconocimiento facial en el contenido de esas bases de datos. Este informe indicó que la tecnología se había desarrollado desde la decisión del Tribunal Supremo. Explicó que la PND [*Police National Database*] está diseñada para facilitar el intercambio de inteligencia. La función de búsqueda facial de la PND permite a un usuario autorizado (generalmente un oficial de policía) buscar a través de las imágenes de custodia guardadas en la PND contra una imagen que han cargado temporalmente desde su base de datos local. Según la Revisión, las fuerzas policiales en Irlanda del Norte también realizan tales búsquedas a través de la PND" (párrafo 68).

"En respuesta a la pregunta del Tribunal sobre la comunicación del caso acerca de la funcionalidad de la base de datos en Irlanda del Norte, el Gobierno confirmó la conclusión del informe del Ministerio del Interior. Indicó que la fotografía del solicitante se mantenía en una base de datos local que no tenía software de reconocimiento facial o mapeo facial, pero que las fotografías de esa base de datos pueden cargarse en la PND, que sí tiene dicho software" (párrafo 69).

"El Tribunal recuerda que, al considerar si ha habido una interferencia, tendrá debidamente en cuenta el contexto específico en el que se ha registrado y retenido la información en cuestión, la

naturaleza de los registros, la forma en que se utilizan y procesan estos registros y los resultados que se pueden obtener. En el presente caso, dado que la fotografía de custodia del solicitante se tomó en el momento de su arresto y se mantendrá indefinidamente en una base de datos local para uso de la policía y que la policía también puede aplicar técnicas de reconocimiento facial y mapeo facial a la fotografía, el Tribunal no tiene dudas de que la toma y retención de la fotografía del solicitante constituye una interferencia con su derecho a la vida privada en el sentido del artículo 8 apartado 1" (párrafo 70).

2. Derechos Humanos. Reglamentación de los derechos. Política criminal. Principio de proporcionalidad. Control de legalidad. Razonabilidad.

"Se debe dejar un margen de apreciación a las autoridades nacionales competentes en esta evaluación. La amplitud de este margen varía y depende de varios factores, incluyendo la naturaleza del derecho del Convenio en cuestión, su importancia para el individuo, la naturaleza de la interferencia y el objeto perseguido por la interferencia. El margen tenderá a ser más estrecho cuando el derecho en juego sea crucial para el disfrute efectivo de los derechos íntimos o clave del individuo. Cuando esté en juego una faceta particularmente importante de la existencia o identidad de un individuo, el margen permitido al Estado será restringido. Sin embargo, cuando no haya consenso dentro de los Estados miembros del Consejo de Europa, ya sea en cuanto a la importancia relativa del interés en juego o en cuanto a la mejor manera de protegerlo, el margen será más amplio" (párrafo 77).

"El Gobierno ha presentado tres razones en relación tanto con la retención de datos biométricos como de fotografías, para explicar por qué el margen de apreciación disponible para el Estado es amplio en el presente caso, basándose en el grado de consenso entre los Estados contratantes. Primero, que no existe consenso entre los Estados sobre cómo abordar la retención de los datos biométricos de personas condenadas por un delito. Segundo, que el esquema de retención en Irlanda del Norte no es inusualmente intrusivo, ya que varias otras jurisdicciones europeas retienen datos biométricos, en algunos casos incluyendo muestras de ADN de personas condenadas, indefinidamente o por periodos muy largos de tiempo, como la vida de la persona en cuestión. Tercero, que el esquema en Irlanda del Norte significa que las muestras solo se tomarán de personas condenadas por delitos registrables, es decir, delitos que son punibles con pena de prisión. En consecuencia, el régimen de retención tiene en cuenta un grado mínimo de gravedad en relación con la delincuencia" (párrafo 78).

"La presentación del Gobierno de que no existe consenso entre los Estados contratantes sobre cómo abordar la retención de los datos biométricos de personas condenadas por un delito, se basa en la suposición de que un régimen que prevé la retención durante la vida biológica, o la vida biológica más un cierto número de años, es comparable a un régimen de retención indefinida. Sin embargo, el Tribunal considera que al concluir si esos dos tipos de régimen pueden equipararse, se debe tener en cuenta la naturaleza de los datos y el impacto de retener los datos de una persona después de su muerte" (párrafo 79).

"En relación con las huellas dactilares, el Tribunal ha encontrado previamente que no contienen tanta información como los perfiles de ADN (véase *S. y Marper*). Además, no se ha sugerido que sea posible identificar relaciones entre individuos a partir de datos de huellas dactilares o fotografías. Por lo tanto, el Tribunal acepta que, en relación con las huellas dactilares y fotografías, los períodos de retención que terminan en o poco después de la muerte podrían considerarse comparables a la retención indefinida; aunque es consciente de la posibilidad de rápidos avances tecnológicos en este dominio, en particular en lo que respecta a la tecnología de reconocimiento facial y mapeo facial. Dicho esto, para las huellas dactilares y las fotografías, la mayoría de los

Estados encuestados han establecido regímenes con períodos de retención definidos" (párrafo 80).

"[E]l Tribunal considera que la situación es diferente en lo que respecta a los perfiles de ADN y que existe una distinción entre retener perfiles de ADN indefinidamente y establecer un límite definido en el período de retención vinculado a la vida biológica de la persona en cuestión, incluso si el período de retención previsto es largo. Esto se debe a que la retención de datos genéticos después de la muerte del sujeto de los datos continúa afectando a los individuos biológicamente relacionados con el sujeto de los datos. El Tribunal recuerda que, al considerar la naturaleza de la interferencia con la privacidad ocasionada por la retención de perfiles de ADN, ha observado que el uso de perfiles de ADN para la búsqueda familiar con el fin de identificar una posible relación genética entre individuos es de naturaleza altamente sensible y existe la necesidad de controles muy estrictos a este respecto. En opinión del Tribunal, la capacidad de los perfiles de ADN para proporcionar un medio de identificar las relaciones genéticas entre individuos es en sí misma suficiente para concluir que su retención interfiere con el derecho a la vida privada de los individuos en cuestión. La frecuencia de las búsquedas familiares, las salvaguardias asociadas y la probabilidad de perjuicio en un caso particular son irrelevantes a este respecto" (párrafo 81).

"Es cierto que en *S. y Marper* [...] el Tribunal encontró que el Reino Unido estaba solo en retener indefinidamente el ADN de personas no condenadas y concluyó que el fuerte consenso existente entre los Estados Contratantes era de considerable importancia y estrechaba el margen de apreciación dejado al Estado demandado en la evaluación de los límites permisibles de la interferencia con la vida privada en esta esfera (véase *S. y Marper*). La situación no es exactamente la misma en el presente caso donde, incluso teniendo en cuenta la distinción identificada entre la retención vinculada a la muerte del sujeto de los datos y la retención indefinida en relación con los perfiles de ADN, hay un pequeño número de estados entre los encuestados que operan regímenes de retención indefinida. No obstante, el Tribunal considera que esos estados están en una clara minoría. La mayoría de los Estados tienen regímenes en los que hay un límite definido en el período durante el cual se pueden retener los datos. También tiene en cuenta el hecho de que el Gobierno, en sus presentaciones, se refirió a esquemas que permiten la retención indefinida de datos biométricos de personas condenadas en Austria y Lituania. Sin embargo, esos regímenes han sido posteriormente modificados para proporcionar períodos definidos de detención" (párrafo 82).

"El Gobierno presentó una presentación separada relacionada con el margen de apreciación, que era que el esquema en Irlanda del Norte significa que las muestras de ADN solo se tomarán (y por lo tanto los perfiles de ADN solo se retendrán) de personas condenadas por delitos registrables, es decir, un delito que es punible con pena de prisión. En consecuencia, el régimen de retención tiene en cuenta un grado mínimo de gravedad en relación con la delincuencia. El Tribunal observa que la Gran Sala rechazó previamente una presentación similar en *S. y Marper*, donde el hecho de que los datos solo se tomaran y por lo tanto se retuvieran en relación con delitos registrables bajo el esquema examinado, todavía dejaba una variedad tan amplia de delitos cayendo dentro del régimen de retención que el régimen podía caracterizarse como aplicándose independientemente de la naturaleza o gravedad del delito (véase *S. y Marper*). El Tribunal no ve razón para adoptar un enfoque diferente al de la Gran Sala" (párrafo 83).

"[E]l Tribunal no puede concluir que el margen de apreciación del Estado se amplíe en el presente caso en la medida reclamada por el Gobierno. El Reino Unido es una de las pocas jurisdicciones del Consejo de Europa que permite la retención indefinida de perfiles de ADN, huellas dactilares y fotografías de personas condenadas. El grado de consenso existente entre los Estados Contratantes ha estrechado el margen de apreciación disponible para el Estado demandado, en

particular con respecto a la retención de perfiles de ADN por las razones expuestas anteriormente" (párrafo 84).

3. Razonabilidad. Principio de proporcionalidad. Control judicial. Derecho de defensa. Política criminal. Derecho a la privacidad.

"En cuanto a si las razones aducidas por las autoridades nacionales para justificar la medida de retención indefinida eran 'relevantes y suficientes', el Tribunal observa que el Gobierno argumentó que cuantos más datos se retienen, más delitos se previenen, proporcionando una variedad de diferentes estudios de casos para apoyar esa afirmación general. A este respecto, el Tribunal considera que aceptar tal argumento en el contexto de un esquema de retención indefinida equivaldría en la práctica a justificar el almacenamiento de información sobre toda la población y sus parientes fallecidos, lo que sin duda sería excesivo e irrelevante (véase *M.K. v. Francia y Aycagauer*). El Tribunal también observa en ese sentido que el Gobierno destacó que aquellos que habían sido condenados eran de hecho más propensos a ser condenados nuevamente después de un período relativamente corto de dos años" (párrafo 89).

"El Tribunal recuerda en términos generales que ha encontrado en el contexto de la obligación positiva que surge del artículo 2 que el interés público en investigar y posiblemente obtener el enjuiciamiento y condena de los perpetradores de homicidios ilegales muchos años después de los hechos está firmemente reconocido (véase *Jelić v. Croacia*). Investigar 'casos fríos' [cold cases], también es de interés público, en el sentido general de combatir el crimen. Sin embargo, también en el contexto de los homicidios ilegales, el Tribunal ha subrayado que la policía debe cumplir sus deberes de una manera compatible con los derechos y libertades de otros individuos (véase *Osman v. el Reino Unido*). De hecho, sin respeto por la proporcionalidad requerida vis-à-vis los objetivos legítimos asignados a tales mecanismos, sus ventajas se verían superadas por las graves violaciones que causarían a los derechos y libertades que los Estados deben garantizar bajo la Convención a las personas bajo su jurisdicción (véase *Aycaguer*)" (párrafo 93).

"Habiendo optado por implementar un régimen de retención indefinida, era necesario que el Estado garantizara que ciertas salvaguardias estuvieran presentes y fueran efectivas para el solicitante, alguien condenado por un delito. Sin embargo, los datos biométricos y las fotografías del solicitante se retuvieron sin referencia a la gravedad de su delito y sin tener en cuenta ninguna necesidad continua de retener esos datos indefinidamente. Además, la policía está investida con el poder de eliminar datos biométricos y fotografías solo en circunstancias excepcionales. No existe ninguna disposición que permita al solicitante solicitar que se eliminen los datos que le conciernen si la conservación de los datos ya no parece necesaria en vista de la naturaleza del delito, la edad de la persona en cuestión, el tiempo transcurrido y la personalidad actual de la persona (véase *Gardel v. Francia*). En consecuencia, la revisión disponible para el individuo parecería ser tan estrecha como para ser casi hipotética (véase *M.K. v. Francia*)" (párrafo 94).

"[E]n cuanto, a las fotografías, el Tribunal considera de interés que el régimen en Inglaterra y Gales se modificó después de RMC para permitir a las personas condenadas por delitos registrables menos graves, solicitar la eliminación de sus fotografías después de seis años, con una presunción de eliminación. Sin embargo, subraya que la prueba de proporcionalidad no consiste en que se pueda imponer otro régimen menos restrictivo. La cuestión central es si, al adoptar la medida y establecer el equilibrio que hizo, el legislador actuó dentro del margen de apreciación que se le otorgó (véase *Animal Defenders International v. el Reino Unido*)" (párrafo 95).

"[E]l Tribunal considera que la naturaleza indiscriminada de las facultades de retención del perfil de ADN, las huellas dactilares y la fotografía del solicitante como persona condenada por un delito, incluso si está cumplido, sin referencia a la gravedad del delito o a la necesidad de retención

indefinida y en ausencia de cualquier posibilidad real de revisión, no logró alcanzar un equilibrio justo entre los intereses públicos y privados en competencia. El Tribunal recuerda su conclusión de que el Estado retuvo un margen de apreciación ligeramente más amplio con respecto a la retención de huellas dactilares y fotografías. Sin embargo, ese margen ampliado no es suficiente para concluir que la retención de tales datos podría ser proporcional en las circunstancias, que incluyen la falta de cualquier salvaguardia relevante, incluida la ausencia de cualquier revisión real" (párrafo 96).

“[E]l Estado demandado ha rebasado el margen de apreciación aceptable a este respecto y la retención controvertida constituye una injerencia desproporcionada en el derecho del demandante al respeto de su vida privada y no puede considerarse necesaria en una sociedad democrática” (párrafo 97).

5.6. TRIBUNAL EUROPEO DE DERECHOS HUMANOS (TEDH), "SABER v. NORUEGA". CASO N° 459/18. 17/3/2021.

HECHOS

Un ciudadano noruego denunció a dos personas por presuntamente conspirar para asesinarlo, lo que llevó al Servicio de Policía de Oslo (SPO) a incautar su teléfono celular para investigar la situación. Considerándolo víctima y parte perjudicada, decidieron realizar una copia espejo del contenido del dispositivo para examinar posibles evidencias relacionadas con el conflicto entre las partes involucradas. Durante el análisis del teléfono, se descubrieron comunicaciones entre el denunciante y sus abogados defensores en otro caso en el que era sospechoso de haber cometido un delito distinto. Ante este hallazgo, la fiscalía solicito que un tribunal local examinara la información recogida y decidiera qué partes de los datos que contenía estaban sujetas al privilegio legal profesional (LPP) y cuales otras podían entregarse a la policía para que las registrara. Al mismo tiempo, la Fiscalía renunció a incautar la correspondencia entre el denunciante y sus abogados, reconociendo su carácter confidencial. Sin embargo, el tribunal local convocó a la fiscalía y a la defensa para discutir el tratamiento de la evidencia obtenida. La defensa expresó su preocupación por la confidencialidad de las comunicaciones presentes en el teléfono entre su defendido con otros abogados. El tribunal decidió establecer palabras clave para filtrar la información, contando con la asistencia de un técnico del Servicio de Policía de Oslo. Sin embargo, como el tribunal carecía de recursos técnicos, buscó asistencia externa. La defensa objetó esta medida, solicitó una decisión formal sobre el proceso de búsqueda de datos. Para ello, argumentó que existía un riesgo de violación del derecho a la privacidad y a la protección de datos personales. Por su parte, la Fiscalía expresó su preocupación por una posible manipulación de pruebas por parte de terceros. En este contexto, y basándose en un caso similar resuelto por la Corte Suprema, solicitó la devolución de la copia espejo para un examen más detenido que permitiera determinar qué partes debían quedar exentas de incautación. El tribunal fundamentó su decisión en una reciente sentencia de la Corte Suprema. En ese sentido, sostuvo que era la policía quien debía realizar ese tipo de filtrado. En consecuencia, devolvió la copia espejo a la policía para su examen y evaluación. El denunciante apeló esta decisión ante el Tribunal Superior. Sostuvo que tenía derecho a que el tribunal local realizara el procedimiento de filtrado. Sin embargo, el Tribunal Superior rechazó el pedido. Para ello consideró que la policía tenía la competencia primaria para tomar decisiones sobre incautaciones y la responsabilidad de garantizar que no se incautaran datos protegidos por el Código Procesal Penal. Posteriormente, el denunciante presentó un recurso ante la Corte Suprema. Sin embargo, el Comité de Apelaciones de la Corte rechazó por unanimidad la apelación.

Entonces, al agotar todas las vías de recurso internas, el denunciante presentó una solicitud ante el Tribunal Europeo de Derechos Humanos en diciembre de 2017. En su solicitud, argumentó que permitir a la policía realizar un examen preliminar de su teléfono inteligente para filtrar datos que podrían estar protegidos por el secreto profesional violaba su derecho al respeto de la correspondencia.

DECISIÓN

El Tribunal Europeo de Derechos Humanos, por mayoría, consideró que Noruega era responsable por la violación del artículo 8 del Convenio Europeo de Derechos Humanos al respeto de su vida privada.

ARGUMENTOS

1. Derecho a la privacidad. Allanamiento. Procedimiento policial. Control judicial. Prueba. Prueba digital. Principio de legalidad. Tipicidad. Orden judicial. Secreto profesional. Regla de exclusión.

"El Tribunal observa de entrada que es indiscutible entre las partes que el registro del teléfono inteligente del demandante y/o de la copia en espejo del dispositivo, supuso una injerencia en su derecho al respeto de su correspondencia en virtud del artículo 8, párrafo primero, del Convenio, y considera que esto no puede cuestionarse (véase, por ejemplo, *mutatis mutandis*, *Laurent v. Francia*). Además, el Tribunal señala que el registro se llevó a cabo hacia el demandante en su calidad de parte agraviada en la investigación pertinente" (párrafo 48).

"En cuanto a la cuestión de si la injerencia fue conforme a Derecho [...], el Tribunal observa que las decisiones relativas al registro como tal y, en última instancia, a cualquier incautación de datos del teléfono del demandante, tenían un fundamento jurídico formal, a saber, en las disposiciones sobre registros del capítulo 15 y las relativas a incautaciones del capítulo 16 del Código Procesal Penal local. En la medida en que se había establecido que el acceso a la correspondencia entre el demandante y sus abogados podía obtenerse a través de la copia espejo de su teléfono inteligente, el *quid* del asunto es, sin embargo, si la ley en cuestión tenía suficiente calidad y ofrecía suficientes salvaguardias para garantizar que el LPP no se viera comprometido durante el procedimiento de registro e incautación" (párrafo 49).

"El Tribunal reitera que el artículo 8 apartado 2 del Convenio exige que la ley en cuestión sea ´compatible con el Estado de Derecho´. En el contexto de los registros e incautaciones, la legislación nacional debe proporcionar cierta protección al individuo contra la injerencia arbitraria en los derechos del artículo 8. La legislación nacional debe ser lo suficientemente clara en sus términos para ofrecer a los ciudadanos una indicación adecuada de las circunstancias y condiciones en las que las autoridades están facultadas para recurrir a tales medidas. Además, el registro y la incautación representan una grave injerencia en la vida privada, el domicilio y la correspondencia, por lo que deben basarse en una ´ley´ especialmente precisa. Es esencial disponer de normas claras y detalladas en la materia (véase *Sallinen y otros v. Finlandia*)" (párrafo 50).

"El Tribunal ha reconocido la importancia de las garantías procesales específicas cuando se trata de proteger la confidencialidad de los intercambios entre los abogados y sus clientes y del LPP (véanse, entre otras, las sentencias *Sommer v. Alemania*, y *Michaud v. Francia*). Ha subrayado que el privilegio legal profesional es la base de la relación de confianza existente entre un abogado y su cliente y que la salvaguarda del secreto profesional es, en particular, el corolario del derecho del cliente de un abogado a no autoinculparse, lo que presupone que las autoridades tratan de probar su caso sin recurrir a pruebas obtenidas mediante métodos de coacción u opresión, desafiando la voluntad de la ´persona imputada´ (véase, por ejemplo, *André y otro v. Francia*). Sin embargo, en su jurisprudencia, el Tribunal ha distinguido entre la cuestión de si se ha violado el artículo 8 con respecto a las medidas de investigación y la cuestión de las posibles ramificaciones de una conclusión en ese sentido sobre los derechos garantizados en virtud del artículo 6 (véase, por ejemplo, entre muchas otras, *Dragoș Ioan Rusu v. Rumania*; y *Dumitru Popescu v. Rumania*). Además, el Tribunal ha subrayado que es evidente que redunda en el interés general que toda persona que desee consultar a un abogado pueda hacerlo libremente en condiciones que favorezcan una conversación plena y sin inhibiciones y que, por esa razón, la relación entre abogado y cliente es, en principio, privilegiada. No ha limitado esta consideración únicamente a las cuestiones relativas a litigios pendientes y ha subrayado que, ya sea en el marco de una asistencia para un litigio civil o penal o en el marco de la búsqueda de asesoramiento jurídico general, las personas que consultan a un abogado pueden esperar razonablemente que su comunicación sea privada y confidencial (véase, por ejemplo, *Altay v. Turquía*)" (párrafo 51).

“Pasando a las circunstancias del presente asunto, el Tribunal observa, en primer lugar, que existía acuerdo en que la copia espejo del dispositivo móvil del demandante contenía mensajes entre él y sus abogados. Observa asimismo que el Código Procesal Penal no contenía ninguna disposición expresa destinada en un principio a prescribir el procedimiento para tales situaciones en las que pudiera estar en juego el LPP. No obstante, la policía y el demandante coincidieron inicialmente en que, para garantizar que no se vulnerara el LPP, los datos de la copia espejo debían ser filtrados por la corte local y cualquier dato del LPP eliminado antes de que la policía pudiera registrar el resto. La base jurídica de este procedimiento sería una aplicación por analogía del artículo 205, apartado 3, de la normativa procesal. La corte local parece haber compartido esta interpretación y procedió en consecuencia para que se hiciera efectivo el filtrado. No obstante, a falta de normas expresas y específicas en la materia, hubo un desacuerdo posterior sobre la forma en que la corte local podía proceder en términos prácticos, incluida la posibilidad de solicitar ayuda a la policía” (párrafo 52).

“[M]ientras la corte local procedía filtrar los datos, la Corte Suprema dictó una sentencia en un caso totalmente ajeno en el que el demandante no había intervenido, en la que se indicaba que era ese tribunal —en contra de lo que suponía el demandante, la policía y la corte local— el que debía filtrar los datos, al parecer porque la Corte Suprema había considerado que era más pertinente otra analogía que la que hasta entonces se consideraba correcta en el presente caso, a saber, la aplicación por analogía de los procedimientos relativos a los datos de vigilancia. Tras recabar la opinión de las personas implicadas en el caso de la demandante sobre esta nueva decisión, la corte local concluyó que, debido a las nuevas indicaciones de la Corte Suprema, debía abandonar su procedimiento de filtrado y devolver la copia espejo a la policía. Posteriormente, la propia policía la examinó” (párrafo 53).

“Habida cuenta de las observaciones precedentes, el Tribunal no considera necesario examinar en el presente asunto si, y en qué circunstancias, las reclamaciones verosímiles por la protección del secreto profesional relativas a determinados soportes de datos implican que éstos deban ser enviados a un tribunal o a un tercero independiente de la policía y de la fiscalía para que se supriman los datos cubiertos el secreto profesional ante de que ésta pueda proceder al registro de los soportes de datos. En el presente asunto, basta con que el Tribunal formule las siguientes observaciones” (párrafo 54).

“En primer lugar, el Tribunal toma nota de la circunstancia de que los procedimientos relativos al filtrado del LPP en casos como el presente carecían desde el principio de una base clara en el Código Procesal Penal lo que los hacía susceptibles de controversias como la que siguió a la decisión de la Corte Suprema. En segundo lugar, la forma real del procedimiento difícilmente podía ser previsible para el demandante, a pesar de que se le permitió oponerse, dado que se reorganizó efectivamente a raíz de esa decisión. En tercer lugar, y lo que es más importante, el Tribunal considera que el Gobierno no ha refutado la alegación del demandante de que, con posterioridad a la conclusión de la Corte Suprema que la policía debía examinar por sí misma los soportes de datos en casos como el presente, la decisión de aplicar esa instrucción al caso en curso del demandante, que adquirió firmeza con la sentencia de la Corte Suprema, significaba que no existían garantías procesales claras y específicas para evitar que el LPP se viera comprometida por el registro de la copia espejo de su teléfono. La Corte Suprema no había dado ninguna instrucción sobre la forma en que la policía debía llevar a cabo la tarea de filtrar el LPP, aparte de indicar que las palabras de búsqueda debían decidirse en consulta con el abogado; a pesar de que la reclamación presentada por el LPP en el presente caso era como tal indiscutiblemente válida, la copia espejo fue efectivamente devuelta sin más a la policía para su examen sin que existiera ningún esquema procesal práctico a tal efecto. En un informe anterior se describe la supresión de datos en el caso del demandante, pero no se describe ninguna base o forma clara para el procedimiento” (párrafo 55).

“[E]l Tribunal subraya que ha tomado nota de que el Gobierno señaló efectivamente las garantías procesales existentes en materia de registros e incautaciones en general; la preocupación del Tribunal es, sin embargo, la falta de un marco establecido para la protección del LPP en casos como el presente. En ese sentido, el Tribunal observa que la Corte Suprema también señaló la falta de disposiciones adaptadas a las situaciones en las que los datos LPP forman parte de lotes de datos almacenados digitalmente, e indicó que sería natural regular la cuestión exacta que se planteó en el presente asunto mediante disposiciones formales conforme a Derecho. Así pues, el Tribunal señala que la cuestión que se planteó en el presente asunto no se debió como tal a las conclusiones de la Corte Suprema en dicho caso, sino que tuvo su origen en la falta de una regulación adecuada, como señaló dicha Corte” (párrafo 56).

“Aunque en el caso del demandante no existía tal regulación, el Tribunal no tiene base para decidir si el LPP se vio realmente comprometida en su caso, ni el demandante ha alegado que lo estuviera. Sin embargo, en opinión del Tribunal, la falta de previsibilidad en el presente caso, debida a la falta de claridad del marco jurídico y a la falta de garantías procesales relativas concretamente a la protección del LPP, ya no cumplía los requisitos derivados del criterio de que la injerencia debe ser conforme a Derecho en el sentido del artículo 8, apartado 2, del Convenio. Una vez extraída esta conclusión, no es necesario que el Tribunal examine el cumplimiento de los demás requisitos exigidos por dicha disposición” (párrafo 57).

5.7. TRIBUNAL EUROPEO DE DERECHOS HUMANOS (TEDH), "SÄRGAVA V. ESTONIA". CASO N° 698/19. 16/11/2021.

HECHOS

La Junta de Policía y Guardia de Fronteras (PBGB) de Estonia estaba investigando a un abogado por su presunta implicación en un delito. En el transcurso de esta investigación, la fiscalía solicitó la autorización para llevar a cabo un registro en su domicilio y vehículos, argumentando sospechas de participación en la elaboración de documentos relacionados con actividades delictivas. En su petición, la fiscalía detalló las actividades sospechosas, justificando la necesidad de obtener información relevante sobre las comunicaciones y transacciones entre los miembros de la presunta organización criminal. El objetivo era recabar cualquier dato almacenado en diversos dispositivos pertenecientes al individuo investigado, como memorias USB, tarjetas de memoria, discos duros, computadoras y teléfonos celulares. El juzgado de instrucción accedió a la solicitud de la fiscalía, autorizando el registro en el domicilio del abogado, su bufete y también la inspección de su vehículo. Además, ordenó su detención como sospechoso por un período de cuarenta y ocho horas. Al día siguiente, la persona fue detenida y su teléfono celular fue secuestrado. Ese mismo día se llevaron a cabo registros tanto en su domicilio como en su bufete de forma simultánea, en los que se secuestró una computadora portátil. Posteriormente, la PBGB realizó copias del contenido del teléfono celular y del disco duro de la computadora portátil. También solicitó al bufete de abogados que proporcionara cualquier información relacionada con las actividades del abogado y dos sospechosos adicionales, así como cualquier vínculo con empresas relacionadas. Sin embargo, el bufete señaló que no podía divulgar información sobre los servicios prestados debido a un acuerdo de confidencialidad entre las partes. Un mes después de la incautación, el abogado solicitó a la PBGB que no se examinaran su teléfono celular y computadora portátil. Asimismo, que el material copiado no se utilizara como evidencia y que se eliminaran todos los datos que pudieran haberse copiado. No obstante, la PBGB rechazó esta solicitud. Entonces, el abogado presentó una queja ante la Fiscalía General. Para ello, solicitó que la incautación sea declarara ilegal. El Fiscal del Estado desestimó la queja. Esta decisión fue recurrida. Sin embargo, el Fiscal Jefe de Estado confirmó el rechazo. Posteriormente, el abogado presentó otra apelación ante el Tribunal del Condado de Harju. Este tribunal desestimó la solicitud. Para ello, señaló que la inviolabilidad de los dispositivos de almacenamiento de datos de los abogados no era absoluta y solo se aplicaba en la medida en que el abogado no cometiera un delito en el marco de la prestación de servicios legales. Además, que esa decisión era inapelable.

Entonces, al agotar todas las vías de recurso internas, el abogado presentó una solicitud ante el Tribunal Europeo de Derechos Humanos en diciembre de 2018. En su solicitud argumentó que la incautación y el posterior examen de su computadora portátil y teléfono móvil violaban el derecho al respeto de la correspondencia.

DECISIÓN

El Tribunal Europeo de Derechos Humanos, por mayoría de cuatro votos contra tres, consideró que Estonia era responsable por la violación del artículo 8 del Convenio Europeo de Derechos Humanos relativo al secuestro y examen de la computadora personal y el teléfono móvil del demandante.

ARGUMENTOS

1. Ley. Principio de legalidad. Arbitrariedad. Control judicial. Orden judicial. Ley. Debido proceso. Abogado. Violación de secretos. Secreto profesional. Allanamiento. Prueba. Prueba digital. Prueba informática.

"En cuanto a la cuestión de si la medida fue conforme a derecho, la jurisprudencia de la Corte ha establecido que una medida debe tener algún fundamento en el derecho interno, entendiéndose el término ´ley´ en su sentido ´sustantivo´ más que en su sentido ´formal´. En el ámbito comprendido por el *statutory law*, la´ley´ es la disposición vigente tal como la han interpretado los tribunales competentes. Además, el derecho interno debe ser compatible con el Estado de derecho y accesible a la persona interesada, y la persona afectada debe poder prever las consecuencias del derecho interno para él o ella (véase *Big Brother Watch y otros v. el Reino Unido*; *Wolland v. Noruega*; véase también *Golovan v. Ucrania*)" (párrafo 86).

"En el contexto de los registros e incautaciones, el derecho interno debe brindar cierta protección al individuo contra la interferencia arbitraria con los derechos del artículo 8. Por lo tanto, debe ser lo suficientemente claro en sus términos para dar a los ciudadanos una indicación adecuada sobre las circunstancias y condiciones bajo las cuales las autoridades están facultadas para recurrir a tales medidas (ver *Golovan*)" (párrafo 87).

"[E]l Tribunal ha reconocido la importancia de garantías procesales específicas cuando se trata de proteger la confidencialidad de los intercambios entre abogados y sus clientes (ver *Sabre v. Noruega* y *Sommer v. Alemania*; véase también *Kadura y Smaliy v. Ucrania*)" (párrafo 88).

"El Convenio no prohíbe imponer a los abogados determinadas obligaciones que puedan afectar a las relaciones con sus clientes. Este es el caso, en particular, cuando se encuentran pruebas creíbles de la participación de un abogado en un delito o en relación con los esfuerzos para combatir determinadas prácticas. Sin embargo, por este motivo es vital establecer un marco estricto para tales medidas, ya que los abogados ocupan una posición vital en la administración de justicia y pueden, en virtud de su papel como intermediarios entre los litigantes y los tribunales, ser descritos como funcionarios de la ley (ver *André y otro v. Francia*)" (párrafo 89).

"Volviendo al presente caso, el Tribunal acepta que se puede decir que la interferencia tuvo una base jurídica general en el derecho interno, a saber, el artículo 91 del Código Procesal Penal" (párrafo 90).

"El Tribunal examinará más a fondo la ´calidad´ de las normas jurídicas aplicables al demandante en el presente caso. Al hacerlo, abordará en primer lugar la cuestión de si el derecho interno es suficientemente claro en lo que respecta a la (in)capacidad de invocar el privilegio profesional jurídico en circunstancias en las que un abogado es sospechoso de haber participado en un delito. En segundo lugar, la Corte examinará si el derecho interno proporciona las garantías procesales necesarias para la protección de la confidencialidad de los intercambios entre abogados y sus clientes" (párrafo 91).

"Pasando al aspecto de las garantías procesales, el Tribunal observa que en el derecho interno existen ciertas garantías en relación con los registros e incautaciones en general, así como con el contexto del registro de estudios jurídicos. De hecho, según el derecho interno, se puede realizar un registro si existe una sospecha razonable de que el objeto se encontrará en el local que se va a registrar. Además, la orden de registro debe especificar en general el objeto, el lugar y los motivos del registro. En caso de que el allanamiento se realice en un despacho de abogados, éste deberá ser autorizado por orden de un juez de instrucción o por orden judicial y el allanamiento deberá realizarse en presencia del abogado cuyo estudio se está allanando o de otro abogado" (párrafo 96).

“El Tribunal observa, sin embargo, que el CCrP [*Code of Criminal Procedure*] no parece exigir la presencia del abogado interesado (u otro abogado) en el caso de que el local que se debe registrar no sea un despacho de abogados sino el domicilio de un abogado o un vehículo o parezca imponer el requisito de autorización judicial en tales circunstancias. No obstante, parece que tales requisitos pueden surgir en virtud del artículo 43(5) de la Ley del Colegio de Abogados. También parece que el derecho interno deja a criterio del juez decidir si autoriza o no el allanamiento mediante una orden plenamente motivada o un aval al pedido de la fiscalía. A pesar de que las autorizaciones en forma de aval son lógicamente más sucintas, no parece que la elección de tal forma haga técnicamente imposible o impida que el juez interno agregue razones o condiciones propias como parte resolutiva de la decisión para autorizar la búsqueda” (párrafo 97).

“A pesar de las garantías antes mencionadas, la preocupación esencial del Tribunal es la falta de un marco práctico para la protección del secreto profesional jurídico en casos como el presente. Partiendo de la premisa de que, según el derecho interno, el privilegio jurídico profesional no se aplica en la medida en que el propio abogado sea sospechoso y/o haya actuado en calidad de abogado, la cuestión clave es cómo se distingue y separa el material privilegiado del material en el que no se puede confiar en la confidencialidad abogado-cliente. El Tribunal observa que esto no se estableció en el procedimiento interno y que claramente no se desprende de las observaciones del Gobierno que, según el derecho interno, la confidencialidad entre abogado y cliente deje de aplicarse por completo con respecto a un abogado que es sospechoso en un caso penal, o que también participa en actividades distintas a la prestación de servicios legales y/o no separa adecuadamente diversos materiales privilegiados y no privilegiados” (párrafo 98).

“Si bien la cuestión de examinar y separar archivos privilegiados y no privilegiados es indudablemente importante en el contexto del material impreso, se vuelve aún más relevante en una situación en la que el contenido privilegiado forma parte de lotes más grandes de datos almacenados digitalmente. En tal situación, incluso si el abogado en cuestión o su representante están presentes en el lugar de búsqueda, podría resultar difícil distinguir rápidamente durante la búsqueda qué archivos electrónicos exactos están cubiertos por el secreto profesional y cuáles no” (párrafo 99).

“La cuestión de cómo llevar a cabo una distinción lo suficientemente selectiva es igualmente pertinente en circunstancias en las que, según la legislación o la práctica nacional, dicha selección no se lleva a cabo en el lugar de la búsqueda, sino que los soportes de datos se incautaron en su totalidad y/o se realiza una copia espejo de su contenido. Sobre ese punto, el Tribunal está dispuesto a aceptar el argumento del Gobierno según el cual la realización de una copia espejo puede considerarse una garantía procesal contra cualquier posible manipulación del contenido de dichos soportes de datos (véase *Wolland*; compárese y (compárese con *Iliya Stefanov v. Bulgaria* y *Kolesnichenko v. Rusia*). Además, una práctica de este tipo permitiría a las autoridades devolver los soportes de datos incautados a sus propietarios con relativa rapidez y, en caso de que los propietarios sean abogados o estudios de abogados, evitaría que su trabajo se vea indebidamente inhibido durante más tiempo del absolutamente necesario” (párrafo 100).

“El Tribunal destaca que la obligación del abogado según el derecho interno (véanse los párrafos 41 a 43 supra) de separar los soportes de datos utilizados en la prestación de servicios jurídicos y la obligación de utilizar estructuras de catálogo claramente marcadas para los archivos de los clientes —si se siguen adecuadamente— contribuiría considerablemente a realizar la tarea de selección de información” (párrafo 101).

“El Tribunal llama la atención sobre el hecho de que además de las garantías que abordan la incautación de soportes de datos y/o la copia de su contenido, así como el filtrado de datos almacenados digitalmente, también es importante evitar el acceso injustificado y no registrado a

los soportes de datos y/o procesamiento de los datos desde el momento de su incautación hasta su devolución o destrucción en su debido momento" (párrafo 102).

"Volviendo a las circunstancias del presente caso, el Tribunal observa que la legislación interna no parece contener ningún procedimiento o garantías específicas para abordar el examen de los soportes electrónicos de datos y evitar que se comprometa la comunicación cubierta por el secreto profesional. El Tribunal considera que esta falta de un sistema procesal práctico y de garantías se refleja, en mayor o menor medida, también en cómo, en el presente caso, se autorizó la búsqueda y en cómo se realizó la copia posterior de los soportes de datos incautados y el examen de su contenido" (párrafo 103).

"En el caso del demandante, la orden de registro emitida por el juez de instrucción no preveía la protección del posible material privilegiado protegido por el secreto profesional (compárese *Kruglov y otros v. Rusia*; *Iliya Stefanov*, citado anteriormente, y *Smirnov v. Rusia*). Esta era la situación a pesar de que la solicitud del Fiscal del Estado de una orden de registro incluía específicamente una referencia a la posibilidad de que el demandante pudiera estar en posesión de información relacionada con sus actividades profesionales como abogado, pero que no sería relevante en el contexto del proceso penal en curso" (párrafo 104).

"Aunque más tarde se aseguró al demandante que la búsqueda del contenido de su ordenador portátil y de su teléfono móvil se realizaría basándose en palabras clave —y dicha búsqueda efectivamente se llevó a cabo—, esta obligación no parecía derivar de la legislación nacional. Por lo tanto, la búsqueda basada en palabras clave no estaba prevista en la solicitud de autorización de búsqueda presentada por el Fiscal del Estado, ni dicha obligación fue mencionada por el juez de instrucción en las órdenes de registro (compárese con *Sérvulo & Associados - Sociedade de Advogados, RL y otros v. Portugal*)" (párrafo 105).

"Más bien, parece que la decisión de realizar una búsqueda basada en palabras clave (o utilizar cualquier otro método de selección), así como la elección de palabras clave relevantes, se dejó enteramente en manos de las autoridades investigadoras. En este punto, el Tribunal observa que algunas de las palabras clave utilizadas para la búsqueda (como ´ejercicio financiero´ o ´línea de crédito´) tenían un alcance notablemente amplio. El Tribunal ya ha determinado anteriormente que el derecho interno no concede al solicitante ningún derecho a estar presente durante la búsqueda basada en palabras clave" (párrafo 106).

"En cualquier caso, la legislación nacional no deja claro cómo se resolverán posibles disputas entre las autoridades investigadoras y el abogado en cuestión sobre las palabras clave que se utilizarán o cualquier otro método para filtrar el contenido electrónico. De hecho, el derecho interno no parece tener normas específicas sobre el procedimiento a seguir en caso de que el abogado o su representante se opongan a la incautación o al examen de contenido en relación con la confidencialidad abogado-cliente (compárese, por ejemplo, *Robathin v. Austria*; *Wieser y Bicos Beteiligungen GmbH v. Austria*; y *André y otro*, citado anteriormente). El Tribunal observa que el derecho interno prevé la posibilidad de interponer un recurso contra las actividades de investigación. Sin embargo, no parece desprenderse del derecho interno que el material respecto del cual se cuestiona la aplicabilidad del secreto profesional no se pondría a disposición de las autoridades investigadoras antes de que los tribunales nacionales hayan tenido la oportunidad de realizar un análisis específico y detallado del asunto y, si es necesario, ordenar la devolución o destrucción de los soportes de datos incautados y/o su contenido copiado (compárese con *Kırdök y otros v. Turquía*; *Vinci Construction y GTM Génie Civil et Services v. Francia*)" (párrafo 107).

"En el contexto de un marco legislativo escaso, el Tribunal considera que la relevancia práctica como garantía de la presencia del abogado en cuestión o de otro abogado durante la búsqueda

—o incluso durante el examen mismo del contenido copiado de los soportes de datos— es de efecto limitado" (párrafo 108).

"Aunque la legislación interna carecía de las garantías procesales adecuadas para proteger los datos cubiertos por el secreto profesional, el Tribunal no tiene base para decidir si la confidencialidad entre abogado y cliente se vio realmente comprometida en el caso que nos ocupa. Sin embargo, en opinión del Tribunal, la falta de garantías procesales relativas específicamente a la protección del secreto profesional ya no cumplía las exigencias que se derivan del criterio de que la injerencia debe ser conforme a la ley en el sentido del artículo 8.2 del Convenio […]. Habiendo llegado a esta conclusión, no es necesario que el Tribunal de Justicia controle el cumplimiento de los demás requisitos previstos en esa disposición" (párrafo 109).

6. PRUEBA DIGITAL OBTENIDA A TRAVÉS DE MEDIOS ILÍCITOS

JURISPRUDENCIA NACIONAL

6.1. CÁMARA FEDERAL DE CASACIÓN PENAL, SALA II. "VAN MEEL, ERIC S/NULIDAD". CAUSA N° 30932. EXPEDIENTE N° 13090/2012. 15/2/2012.

HECHOS

En el marco de una causa penal en la que se investigaba a dos personas, la querella tuvo conocimiento de que tendría lugar una reunión en el salón de un hotel entre las personas imputadas y su defensor. Así, la querella, con la ayuda de otras personas, alquiló el salón colindante, grabó la reunión y luego aportó las desgrabaciones como prueba en el juzgado que investigaba la causa. Posteriormente, la defensa de las personas imputadas cuestionó la validez de las escuchas y grabaciones aportadas por los denunciantes, y solicitó la nulidad de las pruebas obtenidas y ofrecidas. El juez de primera instancia rechazó el pedido de nulidad. Para ello, sostuvo la existencia del principio de amplitud de la prueba procesal; que las reglas del derecho de defensa y la prohibición de obligar al imputado a declarar contra sí mismo no son oponibles a los particulares; que no hubo afectación al derecho de privacidad entre el imputado y su defensor, y que la defensa no pudo explicar de qué modo la grabación y desgrabación de la prueba pudo haber provocado un perjuicio en el ejercicio del derecho de defensa de las personas involucradas. Contra esa decisión, la defensa interpuso un recurso de apelación. Entre otras cuestiones, cuestionó la validez de las conversaciones y grabaciones aportadas por la denunciante.

DECISIÓN

La Sala II de la Cámara Federal de Casación Penal hizo lugar a la impugnación de la defensa, declaró la nulidad y excluyó la prueba ofrecida por la querella (jueces Cattani, Irurzun y Farah).

ARGUMENTOS

1. **Intervención de las telecomunicaciones. Prueba. Prueba informática. Prueba digital. Regla de exclusión. Derecho a la privacidad. Derecho de defensa.**

"[A]mbas Salas de esta Cámara han sostenido que la grabación de una comunicación por parte de uno de sus interlocutores, para el caso de particulares se trata de la documentación de un hecho acaecido que no invade la esfera de las prohibiciones probatorias (Sala I, causa n° 30.468 ´Raña, R. s/nulidad´, reg. n° 255 del 20/4/1999 y Sala II, causa n° 13.928 ´Cingolani y otros s/procesamiento´, reg. n° 15.010 del 19/12/1997). A tal afirmación se le une aquella que sostiene que ´el ocultamiento de dicha filmación sólo ha tenido por objeto la registración por medios técnicos de un hecho que fue realizado libremente por los imputados, quienes asumieron el riesgo de que la oferta ilegal que estaban realizando pudiera ser reproducida ante los tribunales´ (Sala I, causa n° 39.561 ´Leon´, reg. 747 del 11/7/2007 y Sala II, causa n° 26.416 "´Lynch, Santiago y otro s/procesamiento´, reg. n° 28.666 del 8/7/2008)".

"[T]ales supuestos se distinguen del *sub examine*: por un lado [...] porque la parte denunciante que efectuó la grabación no formó parte del círculo de personas que intervinieron en aquella reunión, lo que en sí mismo puede conllevar una indebida intromisión en la privacidad ausente en aquellos casos; y por otro, fundamentalmente por cuanto se trataba de un encuentro entre imputados en una causa penal y su abogado defensor".

"[N]o se encuentra en debate el principio de libertad probatoria y la consecuente validez de la

incorporación al proceso de una grabación efectuada entre particulares, sino que la discusión debe centrarse —conforme lo plantea el incidentista— en si se ha afectado o no la garantía constitucional de inviolabilidad de la defensa".

2. Prueba. Admisibilidad de la prueba. Nulidad. Derecho de defensa.

"[L]a incorporación y valoración de las grabaciones cuestionadas se entromete en un ámbito que diversas disposiciones normativas detraen de toda posible injerencia estatal al hallarse en juego la plenitud del ejercicio de la defensa en causas penales (conf. Sala I, causa n° 30.759 ´Agullo´, reg. n° 481 del 8/7/99)".

"[E]l amparo del secreto profesional está orientado a proteger a la persona que necesita efectuar consultas o requerir asistencia técnica sobre una disciplina en particular —en la especie, jurídica—, para garantizar un ámbito de privacidad y la seguridad de que, a menos que dé un permiso para ello, sus manifestaciones no serán divulgadas (artículo 18 de la Constitución Nacional, artículos 156 y sgtes. del C.P. y 234 y sgtes. del CPPN)".

"[D]ebe interpretarse que las grabaciones en cuestión se ven alcanzadas por tal restricción, dado que, considerar lo contrario, traería aparejado una lesión a la esfera de la reserva e intangibilidad en que debe colocarse la preparación de la defensa penal, acarreando una clara violación a la garantía de defensa en juicio [...]".

"Repárese en la afectación a la plenitud de la defensa en juicio que sobrevendría a raíz de la admisión de pruebas como las cuestionadas, en la medida en que toda comunicación entre un imputado y su círculo íntimo con el abogado se hallaría sujeta a ser incorporada como prueba de cargo".

"La amenaza de tal riesgo recortaría la amplitud del intercambio comunicativo necesario para el desarrollo de toda defensa, con la consiguiente disminución del goce de derechos individuales".

"[E]l Comité de Derechos Humanos de las Naciones Unidas, en su observación n° 13 relativa al artículo 14 del Pacto Internacional de Derechos Civiles y Políticos —análogo al artículo 8 de la Convención Americana sobre Derechos Humanos—, señaló que el defensor debe poder comunicarse con el acusado en condiciones que garanticen plenamente el carácter confidencial de sus conversaciones, y más aún, el poder asesorar y representar a sus clientes de conformidad con su criterio y normas profesionales establecidas, sin ninguna restricción, influencia, presión o injerencia indebida de ninguna parte (conf. Naciones Unidas; Instrumentos Internacionales de Derechos Humanos: publicación del 29 de marzo de 1996, pág. 18)".

"[L]a incorporación de la grabación clandestina conlleva a la imposibilidad de desarrollar la actividad señalada, habiéndose afectado las disposiciones allí establecidas y, por ende, lesionado principios cuyo marco normativo se encuentra en nuestra Carta Magna al integrar la nómina de pactos con jerarquía constitucional, los que deben ser valorados en forma conjunta con los establecidos por el artículo 18 de la Constitución Nacional".

6.2. JUZGADO NACIONAL EN LO CRIMINAL Y CORRECCIONAL N° 5. "ROBLES". CAUSA N° 16/2023. 17/01/2023.

HECHOS

Un abogado particular, a partir de una noticia publicada en un medio local, presentó una denuncia contra un funcionario del Poder Judicial por haber mantenido conversaciones con otro funcionario de la administración pública de la Ciudad de Buenos Aires, por aparentes desvíos de poder. Para sostener la denuncia presentó capturas de pantallas de esas conversaciones y sugirió el secuestro del aparato telefónico del funcionario judicial como medio de prueba. Posteriormente, se habilitó la feria, se dispuso la acumulación y un único trámite. Corrida la vista al Ministerio Público Fiscal, éste indicó que no se encontraba debidamente acreditada la materialidad de los delitos denunciados y resolvió archivar las actuaciones. Para así dictaminar, consideró que no se observaba la existencia de ningún medio o elemento autónomo y autosuficiente distintos de aquellas comunicaciones que podrían haberse sido obtenidas ilícitamente. Por su parte, la defensa consistió en el pedido de archivo de la causa.

DECISIÓN

El Juzgado Nacional en lo Criminal y Correccional N°5 dispuso el archivo de la causa solicitada por el representante del Ministerio Público Fiscal.

ARGUMENTOS

1. **Principio acusatorio. Consentimiento Fiscal. Prueba. Prueba informática. Apreciación de la prueba. Sobreseimiento. Regla de exclusión.**

"[Existe una] obligación constitucional, luego de efectuado un pormenorizado examen de validez del dictamen fiscal, de decidir conforme a lo prescripto por el artículo 180 y 195 del Código de Rito, es decir, archivar la presente denuncia en concordancia con lo propuesto, debido a que no se encuentra habilitada por parte de quien detenta la potestad acusar, la acción penal, y su dictamen es razonable y válido como tal".

"[E]l juez debe velar porque no haya injerencias arbitrarias o ilegales en la vida privada de las personas sin razón que lo justifique, lo que necesariamente implica proteger las comunicaciones como todo aquello que afecte la intimidad de los individuos que conviven en un estado constitucional de derecho (salud, patrimonio, etc.), y en el que se aspira a vivir en un marco democrático, donde el ser humano se pueda desarrollar con plenitud, sin temor a que alguien o el propio Estado, se entrometa en su vida privada de forma ilegal".

"Recomponer [...] el estado constitucional de derecho, llevó y lleva en la actualidad un arduo trabajo, que involucra a la sociedad en su conjunto, de la cual forman parte tanto los funcionarios públicos como aquellos que sobre todo se dedican al derecho, motivo por el que es inadmisible e insostenible, que un proceso se inicie con prueba violatoria a las mínimas garantías e insostenible, que un proceso se inicie con prueba violatoria a las mínimas garantías constitucionales, y/o lo que es peor aún, que pueda ser iniciada a través de la comisión de un delito penal".

"[No] pueden ser admitidas bajo ningún concepto como parte de un juicio respetuoso del debido proceso, pruebas o testimonios que hayan sido obtenidos [...] mediante maniobras organizadas basadas en actividades de inteligencia ilegal".

"[N]o se puede soslayar que al argumento angular del titular de la acción pública [...] radicó en

que las presuntas conversaciones, habrían llegado a oídos de los denunciantes tan solo a través de medios de difusión masiva, y que ellas habrían sido a su vez obtenidas por medio de posibles maniobras de inteligencia ilegal, y/o publicadas o ´filtradas´ por medio informáticos sin consentimiento de alguno de los distintos interlocutores".

"Esta ilegalidad del acto probatorio puede surgir a raíz de: (1) su obtención irregular derivada de una ilegalidad sustantiva con afectación a derechos fundamentales o garantías constitucionales (aquí actúa la llamada regla de exclusión y la doctrina del fruto del árbol venenoso); (2) su incorporación ilegal al proceso derivada de una ilegalidad adjetiva o procesal ya que se aparta de la manera en que se encuentra prescripta formalmente su eficiencia procesal (aquí opera las denominadas sanciones procesales stricto sensu como la nulidad o la inadmisibilidad)".

"[S]e puede proceder según la regla de la exclusión de prueba. Ella tiene como finalidad que la evidencia que haya sido obtenida por medios antijurídicos no pueda ser presentada por la acusación en un juicio criminal".

"[L]a consecuencia de excluir una determinada prueba por haber violado en su recolección derechos fundamentales, es la imposibilidad de valorar el elemento de prueba de modo que el órgano jurisdiccional no pueda basar ninguna de sus futuras decisiones-directa o indirectamente-en una prueba viciada por esas razones".

7. PROTECCIÓN DE DATOS PERSONALES Y LIBERTAD DE EXPRESIÓN EN EL ÁMBITO DIGITAL

JURISPRUDENCIA NACIONAL

7.1. JUZGADO CRIMINAL Y CORRECCIONAL FEDERAL N°11. "ECHEGARAY Y OTROS". CAUSA N°12593/2014. 1/6/2016.

HECHOS

Un hombre sospechado de delitos de asociación ilícita y evasión fiscal denunció a tres representantes de AFIP por el delito de falso testimonio. Durante la investigación, el fiscal amplió la imputación en orden al delito de violación de secretos, por entender que los datos que dieron origen a la causa que se investigan los delitos de asociación ilícita y evasión fiscal, eran confidenciales de acuerdo con lo establecido en el art. 27 del Convenio entre la República Argentina y la República de Francia (Ley 22.357) y solo podían ser usados con fines fiscales.

DECISIÓN

El Juzgado Criminal y Correccional Federal N°11 dictó el procesamiento por considerar a dos imputados coautores del delito de falso testimonio y el otro sujeto como instigador, en concurso real con el delito de violación de secretos en calidad de coautores todos (juez Bonadio).

ARGUMENTOS

1. Violación de secretos. Funcionarios públicos.

"Los datos, de acuerdo con el Convenio [entre la República argentina y la República francesa para evitar la doble imposición y prevenir la evasión fiscal en materia de impuestos sobre la renta y el patrimonio, ley 22.357] eran secretos para todo otro objetivo que no fuese la percepción de impuestos, y eso por eso que la conducta de quienes los emplearon con otros fines encuadra en la figura penal de violación de secretos".

"El objeto de tutela, como en otras figuras del mismo capítulo, es el secreto, pero no cualquiera sino el que tiene origen y debe mantenerse en el ámbito de la administración pública. El acceso por el funcionario es legítimo, no se trata de un caso de intrusión. El núcleo del tipo es la conducta de ´revelar´ a quien no se encuentre comprendido por la obligación de reserva. Vale decir, descubrir o poner de manifiesto a/ante alguien que no pertenece al círculo de habilitados a conocer hechos, actuaciones, documentos o datos que, por ley, deben ser secretos. La revelación no demanda que se difunda o divulgue, o que se concrete un perjuicio material determinado, bastando su sola posibilidad".

7.2. CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL, SALA I. "MINISTERIO PÚBLICO FISCAL S/RECURSO DE APELACIÓN". CAUSA N° 8991/2019. 14/03/2022.

HECHOS

En una causa penal se investigaba a un grupo de personas que se habían desempeñado en el Poder Ejecutivo Nacional entre los años 2015 y 2019 por posibles coacciones orientadas a interferir en las funciones de determinados jueces y juezas. En ese marco, la fiscalía interviniente le solicitó a la Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado de la Corte Suprema de Justicia de la Nación que confeccione un informe en el que se releven todas aquellas manifestaciones directas de carácter público de funcionarios o allegados a la gestión de gobierno que encabezó el Poder Ejecutivo Nacional entre el 10/12/2015 y el 9/12/2019, cuyos contenidos estén emparentados con expresiones de connotaciones críticas, negativas, peyorativas y/o descalificantes, en términos profesionales y/o personales, hacia las personas presuntamente afectadas en el marco de la hipótesis delictiva investigada en aquel caso. Luego de realizado un informe parcial, el juez de primera instancia ordenó excluirlo como medio de prueba. Contra esa decisión, la fiscalía interpuso un recurso de apelación. Para ello, indicó, entre otras cuestiones, que la medida era idónea, válida y respetaba los derechos fundamentales de las personas involucradas en la investigación. Asimismo, que la recolección de datos buscaba determinar la existencia de un hecho criminal en función de que la información no era reservada sino de contenido público, y que la medida no tenía como objetivo censurar expresiones ni judicializar el debate público.

DECISIÓN

La Sala I de la Cámara Nacional de Apelaciones en lo Criminal y Correccional rechazó el recurso de la fiscalía y confirmó la resolución que excluía el informe como medio de prueba.

ARGUMENTOS

1. Debido proceso. Nulidad. Prueba. Derecho de exclusión. Libertad de expresión. Principio de proporcionalidad.

"La medida de prueba así ordenada, aparece ya laminarmente como extralimitada e invasiva de derechos vitales del sistema democrático, tal como la libertad de expresión (art 14 CN), que se encuentran especialmente protegidas por nuestra constitución y merecen particular atención, precaución y tutela por parte de la jurisdicción".

"Cualquier orden de obtención de prueba que pueda afectar las garantías en cuestión debe ser específica y estrictamente limitada, cualidades que no se advierten en la diligencia en análisis. Es especialmente destacable en este sentido la forma indiscriminada en que se produce la apertura de la medida a un análisis global de formas de expresión cualificadas genéricamente y en las que, se destaca especialmente, el adjetivo 'crítica'".

"La afección a un número indeterminado de personas, que incluye hasta una subdivisión indeterminable e inespecífica de 'allegados' —por sobre los ya puntualizados por el momento—, también dan a la medida una inusual extensión que obliga a descalificarla. Afecta no sólo libertades esenciales de los imputados, sino también a la de ilimitadas personas ajenas al proceso, con el consecuente señalamiento social y estigmatización".

“También se observa que la medida infringe normas procesales y constitucionales que hacen a la garantía del debido proceso penal, constituyendo éste, un segundo obstáculo a la pretensión del apelante”.

“La inconstitucionalidad de la diligencia decidida precedentemente no implica que la garantía a expresarse libremente de los ciudadanos adquiera el *status* de un derecho absoluto que anule cualquier limitación legal al respecto. No hay discusión a que toda persona tiene derecho a exteriorizar sus opiniones, pero pueden darse ocasiones en las cuales éstas trasuntan el ámbito de libertad individual, acarreando diversas consecuencias jurídicas”.

“[D]e hallarse conformado este escenario y presumir la posible comisión de un ilícito a través de alguna expresión pública, tampoco resultaría admisible una medida probatoria como la llevada a cabo en autos, caracterizada por su indiscriminada magnitud en cuanto al plazo de tiempo que aborda, las numerosas personas que involucra y la inusitada amplitud de los registros que incluye para análisis, excediendo, asimismo, los límites que razonablemente permite el objeto impuesto por la parte acusadora”.

“[E]n tanto su incorporación al proceso revestida por estas particularidades, vulneraría las cláusulas y garantías de jerarquía constitucional, que exigen que las pruebas ordenadas en el juicio penal se atengan a pautas de necesidad, razonabilidad y proporcionalidad (CSJN, Fallos 341:150; Corte IDH, ´*Caso Escher y otros v. Brasil*´ y su cita del ´*Caso Tristán Donoso v. Panamá*´)´”.

2. Prueba. Principio de proporcionalidad. Deber de fundamentación. Funcionarios públicos.

“[N]o se desconoce que en algunas investigaciones un análisis integral de diversos aspectos puede determinar un hecho delictivo que, estudiados en forma individual o parcializada, no revestirían significación criminal alguna. Tampoco se ignora que el proceso penal, con el fin de llegar a la verdad, cuenta con distintos instrumentos legales que, de manera taxativa, excepcional y bajo el cumplimiento de estrictos requisitos previos (debida fundamentación), permite adoptar medidas que restringen los derechos de las personas imputadas”.

“Pero la viabilidad de estos supuestos no se halla configurada en autos, en tanto el acusador no ha podido investir a su pretensión de una fundamentación suficiente en el sentido expuesto y que respete los requisitos de necesidad, razonabilidad y proporcionalidad referenciados, como para demostrar la excepcional necesidad de llevar a cabo una medida probatoria que —como ya se señaló— quebranta severamente y de manera general importantes garantías constitucionales y cuya producción debe ser evaluada como ´*ultima ratio*´”.

“Del análisis de las actuaciones y específicamente del auto que ordena la medida, no se desprende que ésta resulte ser la única y exclusiva fuente para arribar a una hipótesis criminal concreta-trasladada en un acontecimiento histórico con relevancia jurídico penal), cuando de la prevención del Ministerio Público Fiscal surge que las presuntas amenazas investigadas habrían sido consumadas a través de diversos medios (visitas personales, denuncias, comunicaciones telefónicas), permitiendo ello la adopción de diligencias probatoria alternativas, menos lesivas a la analizada en esta incidencia y mucho más específicas para acreditar los extremos de la hipótesis que el fiscal pretenda sostener”.

“Tampoco la fiscalía ha exteriorizado un razonamiento lógico que permita inferir su relevancia como valor probatorio”.

“La sola mención a ´*declaraciones públicas de rasgos intimidantes*´, ´c*onnotaciones críticas, negativas, peyorativas y/o descalificantes, en términos profesionales y/o personales*´, constituyen parámetros imprecisos y absolutamente subjetivos, que-además de trasladar su determinación al

organismo encargado de efectuar la diligencia, cuando ello constituye una tarea exclusiva e indelegable del director del proceso- impide evaluar la aptitud probatoria de la medida".

"Pero lo más significativo y que coloca a la prueba por fuera del marco de razonabilidad requerido, es que no permite comprender, cuáles serían las características que debe revestir la ´opinión´ para constituir una ´amenaza´ en el sentido que el tipo penal imputado en autos persigue (artículo 149 ter, punto 2, apartado ´a´, del Código Penal)".

"Estas imprecisiones convierten a la medida como difusa y acentúan su ausencia de razonabilidad y pertinencia".

"[N]o puede soslayarse que los sujetos pasivos de la conducta imputada son los funcionarios públicos, los cuales en forma permanente están expuestos a críticas, no sólo por partes de los poderes que componen el Estado, sino por la ciudadanía en su conjunto. Y este ´costo´ conlleva un ´beneficio´ superior, que hace a garantizar la libertad de expresión y a aportar al sistema democrático una herramienta fundamental como lo es el debate lícito de los actos republicanos".

"La medida también desatiende este contexto fáctico, cuando su consideración se evidencia como relevante a los efectos de encauzar un lineamiento investigativo eficaz y razonable, tendiente a corroborar o descartar el hecho imputado en autos".

JURISPRUDENCIA INTERNACIONAL

7.3. CORTE INTERAMERICANA DE DERECHOS HUMANOS, "MIEMBROS DE LA CORPORACIÓN DE ABOGADOS ´JOSÉ ALVEAR RESTREPO (CAJAR) V. COLOMBIA´". 18/10/2023.

HECHOS

El Colectivo de Abogados "José Alvear Restrepo" (CAJAR) era una organización no gubernamental dedicada a la defensa y protección de los derechos humanos en Colombia. Entre 1990 y 2001, miembros de la organización sufrieron hostigamientos, intimidaciones, amenazas y atentados. En particular, denunciaron que funcionarios públicos llevaron a cabo labores de vigilancia, seguimiento, interceptación de comunicaciones, recopilación de información y registros con datos de índole personal, familiar y profesional de integrantes de esta organización y de sus familiares, incluidos sus hijos. Una de las víctimas recibió en su domicilio una muñeca descuartizada y con marcas en sus partes íntimas, alusivas a actos de violencia sexual. En ese contexto, señalaron que las agresiones respondieron a un plan estatal desarrollado a lo largo de los años para inhibir su labor de defensa y protección de los derechos humanos, particularmente en el ámbito judicial e internacional de litigio en casos emblemáticos. A raíz de las denuncias, se iniciaron diversas investigaciones que en su mayoría fueron archivadas o concluidas sin obtener una sanción de las personas responsables.

DECISIÓN

La Corte Interamericana de Derechos Humanos consideró que Colombia era responsable por la violación de los derechos a la vida (artículo 4), a la integridad personal (artículo 5), a la honra (artículo 11), a la libertad de pensamiento y de expresión y a conocer la verdad en relación con el derecho de acceso a la información (artículo 13), a la protección de la familia (artículo 17), de la niñez (artículo 19) y de circulación y residencia (artículo 22) de la Convención Americana sobre Derechos Humanos, en relación con su artículo 1.1. Asimismo, declaró la responsabilidad del Estado por la violación de los derechos a las garantías judiciales (artículo 8.1), a la protección judicial (artículo 25) y a defender los derechos humanos (4.1, 5.1, 8.1, 13.1, 16.1 y 25.1), en relación con el artículo 1.1 del mismo instrumento. Por otra parte, consideró que Colombia era responsable por la violación del derecho a la vida privada (artículo 11) y del derecho a la autodeterminación informativa (artículos 11 y 13) de la CADH, en relación con artículos 1.1 y 2 del mismo instrumento internacional. Por último, consideró que Colombia era responsable por la violación de los derechos a la integridad personal (artículo 5) y la niñez (artículo 19), en relación con las obligaciones de respetar y garantizar los derechos y de abstenerse de cualquier acción o práctica de violencia contra la mujer que establecen los artículos 1.1 de la CADH y el artículo 7.a de la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer.

ARGUMENTOS

1. Actividades de inteligencia. Intervención de las comunicaciones. Control judicial. Derecho a la vida privada y familiar. Libertad de expresión.

"[Es una exigencia que exista un] marco legal [que] defina las actividades de inteligencia, los fines que por su medio deben perseguirse y las facultades de los órganos y autoridades competentes. En tal sentido, se hace imprescindible que una ley regule, con precisión, tales aspectos, cuyo contenido debe ser accesible para el público en general. Esta primera exigencia, coherente con [el] derecho a la vida privada [...] se dirige a evitar que las actividades de inteligencia, lejos de servir a los intereses generales de la sociedad, se constituyan en sí mismas en un riesgo para el

respeto de la dignidad de la persona y sus derechos. Dicha ley, necesariamente promulgada por el Poder Legislativo (ley en sentido formal), debe prever, con la mayor precisión posible, las distintas amenazas que determinan la necesidad de emprender las actividades de inteligencia por parte de los agentes estatales con competencia en la materia, cuyas facultades también deben estar clara y exhaustivamente establecidas, a fin de limitar eficazmente su actuar, impedir la arbitrariedad en su proceder y posibilitar su control y la eventual deducción de responsabilidades" (párrafo 528).

"La necesidad de que la ley sea accesible para el público repercute en que, a diferencia de las actividades de inteligencia propiamente dichas, el marco legal que las autoriza y regula nunca puede ser de carácter reservado, permitiendo así que las personas conozcan las facultades del Estado en este ámbito y, a partir de ello, estén en capacidad de prever que eventualmente tales actividades podrían incidir en su esfera propia de derechos…" (párrafo 530).

"Una segunda exigencia concierne a que las actividades de inteligencia necesariamente habrán de dirigirse a la realización de un fin legítimo. […] De esa cuenta, serán fines legítimos en este ámbito los siguientes: a) la protección de la seguridad nacional; b) el mantenimiento del orden público; c) la salvaguarda de la salud pública, y d) la protección de los derechos humanos…" (párrafo 531).

"[L]a efectiva protección de los derechos a la vida privada y a la libertad de pensamiento y de expresión, sumado al extremo riesgo de arbitrariedad que supone la utilización de las técnicas de vigilancia, selectiva o a gran escala, de las comunicaciones, máxime ante las nuevas tecnologías existentes, determinan para esta Corte que cualquier medida en tal sentido (lo que incluye la interceptación, vigilancia y seguimiento de todo tipo de comunicación, sea telefónica, telemática o por otras redes) exige que sea una autoridad judicial la que decida sobre su procedencia, definiendo a su vez los límites que se imponen, incluidos el modo, tiempo y alcances de la medida autorizada " (párrafo 547).

2. Actividades de inteligencia. Intervención de las comunicaciones. Secreto profesional. Derecho de defensa. Derecho a la autodeterminación informativa.

"[S]e torna imprescindible limitar las acciones de inteligencia respecto de determinadas categorías de personas, particularmente las y los periodistas, en función de salvaguardar la confidencialidad de sus fuentes , y los abogados y las abogadas, a fin de garantizar el secreto de las comunicaciones que mantengan con sus clientes y patrocinados en el marco de su relación profesional [...]. Respecto de las abogadas y los abogados, el artículo 8.2 d) de la Convención Americana reconoce el derecho del inculpado a 'comunicarse libre y privadamente con su defensor', lo que revela el alcance de la protección en torno a la función de dichos profesionales y, a su vez, los límites que se imponen frente a las acciones de inteligencia, dada la importancia de salvaguardar el secreto profesional. Lo anterior deriva no solo del interés por garantizar la protección a la vida privada de las personas, sino, además, por el fin de preservar eficazmente el respeto a las garantías judiciales y al derecho de defensa de quien es representado por la o el profesional jurídico" (párrafos. 555-557).

"Los estándares internacionales refieren también la necesidad de disponer de métodos razonables, ágiles, sencillos, eficaces y gratuitos para que las personas cuyos datos personales han sido recopilados puedan solicitar el acceso, rectificación y eliminación de los datos, así como el derecho a oponerse a su tratamiento y, en lo aplicable, el derecho a su 'portabilidad', es decir, el derecho a recibir los datos 'en un formato estructurado, de uso común y lectura mecánica', si ello fuera factible, pudiendo requerir su transmisión sin que lo impida la autoridad que los gestiona…".

“En el ámbito europeo se reconoce el derecho de las personas a saber si los datos de su titularidad son o no objeto de tratamiento por parte de las autoridades. En su caso, la persona tiene derecho a obtener información sobre (i) los fines y la base jurídica del tratamiento; (ii) las categorías de datos personales de que se trate; (iii) los destinatarios o las categorías de destinatarios a quienes hayan sido comunicados los datos personales, y (iv) el plazo contemplado durante el cual se conservarán los datos personales y los criterios utilizados para determinar dicho plazo. En el caso de información confidencial relacionada con seguridad pública, seguridad nacional o la protección de los derechos humanos, es posible restringir el derecho de acceso del interesado, imponiendo al responsable del tratamiento el deber de justificar por escrito los motivos de la denegación…”.

“A juicio de la Corte Interamericana, los elementos anteriores dan configuración a un derecho humano autónomo: el derecho a la autodeterminación informativa, reconocido en distintos ordenamientos jurídicos de la región, y que encuentra acogida en el contenido tutelar de la Convención Americana, en particular a partir de los derechos recogidos en los artículos 11 y 13, y, en la dimensión de su protección jurisdiccional, en el derecho que garantiza el artículo 25…”.

“[E]l derecho a la autodeterminación informativa participa en la protección a la vida privada que reconoce el artículo 11 de la Convención, en cuanto prohíbe las injerencias arbitrarias o abusivas a esta (numeral 2), y garantiza el amparo ‘de la ley contra esas injerencias’ (numeral 3). A su vez, la autodeterminación informativa se sustenta en el derecho de acceso a la información que esta Corte ha reconocido a partir del contenido del artículo 13.1 de la Convención…”.

“[El derecho a la autodeterminación informativa es] un derecho autónomo que sirve, a su vez, de garantía de otros derechos, como los concernientes a la privacidad, a la protección de la honra, a la salvaguarda de la reputación y, en general, a la dignidad de la persona. Es preciso acotar que el derecho alcanza, con las limitaciones aplicables […], a cualquier dato de carácter personal en poder de todo órgano público, y opera igualmente respecto de registros o bases de datos a cargo de particulares, cuestiones sobre las que no se ahonda en razón del objeto de este proceso internacional…” (párrafos 582-588).

“[E]s factible que los objetivos mismos de las actividades de inteligencia tornen inviable, en determinadas circunstancias, el acceso total o parcial a los archivos de las autoridades. En tales casos, para los efectos de afirmar la compatibilidad con la Convención Americana de cualquier restricción en este ámbito, son útiles, en lo aplicable, los criterios definidos por la jurisprudencia interamericana en materia de limitaciones válidas al derecho de acceso a la información. En tal sentido, lo primero que se exige es que cualquier restricción al derecho, como podría ser la calificación como reservada de la información en poder de las autoridades de inteligencia, debe estar previamente fijada por una ley…”.

“[L]a previsión legal debe ser, en la mayor medida posible, clara y precisa, en el sentido de detallar qué tipo de información o documentos se consideran reservados y cuál es el límite temporal para la reserva. Sin perjuicio de que la autoridad debe garantizar que los datos personales no serán divulgados ni puestos a disposición de terceros en contravención del marco legal, lo que configura una salvaguarda para los derechos del titular de los datos […], el carácter reservado de la información que impida su acceso y control a este último habrá de considerarse siempre excepcional, de manera que la ley debe prever, con especificidad, los motivos para calificar como tal determinada información, en función de su contenido…”.

“En lo que concierne particularmente a la reserva de información personal en poder de los organismos de inteligencia, justificada en el fin de protección de la seguridad nacional, no es factible que el Estado impida el acceso a cualquier información que, mediante una calificación general, se considere relacionada con dicho fin, sino que es necesario que la ley designe las

categorías específicas y estrictas que en función de dicho objetivo son alcanzadas por la reserva. En consecuencia, no resulta compatible con los estándares interamericanos establecer que un documento es reservado por el solo hecho de pertenecer a un organismo de inteligencia y no con base en su contenido…".

"La Corte, en congruencia con los criterios internacionales sobre la materia, identifica los siguientes supuestos concretos que, respondiendo al objetivo de la seguridad nacional, podrían legitimar una regulación legal en tal sentido y, consecuentemente, autorizarían la negativa del Estado a proveer la información solicitada, en poder de los servicios de inteligencia, entre los cuales se encuentran los siguientes: a) información sobre planes de defensa en curso; b) información sobre las capacidades o el uso de sistemas de armamentos o comunicaciones por las fuerzas militares; c) información sobre medidas destinadas al resguardo del territorio o las instituciones nacionales frente a concretas amenazas, siempre que la efectividad de las medidas dependa de su confidencialidad; d) información sobre las operaciones, fuentes o métodos de los servicios de inteligencia concernientes a asuntos de seguridad nacional, y e) información relacionada con asuntos de seguridad nacional suministrada por Estados extranjeros u organismos intergubernamentales, así como comunicaciones diplomáticas sobre tales asuntos, respecto de los cuales exista una expectativa expresa de confidencialidad. Tales supuestos, circunscritos al fin de protección de la seguridad nacional, configuran, a juicio de la Corte, límites válidos y razonables al derecho de acceso a la información y datos personales…".

"La restricción impuesta, según ha exigido la jurisprudencia interamericana, debe cumplirlos requisitos de idoneidad, necesidad y proporcionalidad en las circunstancias del caso concreto. En otras palabras, la reserva de la información contenida en los archivos de inteligencia debe ajustarse a las exigencias del principio de proporcionalidad, esto es: a) que la reserva sea idónea o adecuada para alcanzar el fin que persigue, precisamente, la negativa de posibilitar el acceso a la información; b) que la reserva sea necesaria, por considerarse absolutamente indispensable para alcanzar aquel fin, descartando la existencia de cualquier otra medida menos gravosa para el derecho de acceso a la información que resulte igualmente idónea para la realización del fin perseguido, y c) que la reserva resulte estrictamente proporcional, en el sentido que la limitación al derecho de acceso a la información no se advierta exagerada o desmedida frente a las ventajas que se obtienen por medio de tal limitación y la consecuente realización del fin perseguido […]. Así, la aplicación del test de proporcionalidad en casos concretos puede posibilitar que, garantizando la realización del fin legítimo perseguido, se permita el acceso parcial a determinados archivos, documentos o datos…".

"En cualquier caso, de considerarse inviable la solicitud de acceso y control de los datos, la autoridad competente habrá de dictar una decisión suficientemente motivada, en congruencia con las garantías del debido proceso que vinculan a cualquier autoridad del Estado que pueda afectar derechos (artículo 8.1 de la Convención), en el sentido de justificar de manera clara y completa el fundamento de su negativa…" (párrafos 601-606).

3. Libertad de expresión. Género. Víctimas. Debida diligencia. Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Convención de Belém do Pará).

"Como elemento del debido proceso, la participación de las víctimas en un trámite procesal implica, necesariamente, el acceso al expediente respectivo. Si bien es admisible que en ciertos casos exista reserva de las diligencias adelantadas durante la investigación preliminar en el proceso penal para así garantizar la eficacia de la administración de justicia, en ningún caso puede invocarse dicha reserva para impedir a la víctima el acceso al expediente de una causa penal. Lo mismo ocurre en torno a la reserva que pueda invocarse con base en motivos de seguridad nacional u otra categoría similar respecto de información que conste en las actuaciones, de

manera que, en procura del derecho de las víctimas, la autoridad fiscal o judicial debe garantizar el acceso de estas al expediente, adoptando las medidas necesarias para evitar la difusión indebida de lo que obre en las diligencias…" (párrafo 802).

"La situación que enfrentan las mujeres defensoras ha determinado que sean calificadas como uno de los grupos de personas 'más expuestas al acoso y la persecución' en territorio colombiano, subrayándose la 'dimensión de género de los ataques, amenazas, insultos y prácticas humillantes' efectuadas en su contra. Aunado a ello, se ha destacado que, debido a sus responsabilidades familiares, 'las defensoras se enfrentan a mayores dificultades para trasladar su domicilio a lugares más seguros' en los casos de riesgo para su vida e integridad " (párrafo 882).

4. Libertad de expresión. Libertad de asociación. Protesta. Responsabilidad del Estado.

"[L]a Corte constata [...] la conculcación a la libertad de expresión de las presuntas víctimas en sus labores de promoción, defensa y denuncia en el ámbito de los derechos humanos. En tal sentido, conforme a los fines perseguidos mediante el actuar ilícito de las autoridades estatales, los múltiples hechos perpetrados en perjuicio de los integrantes del Colectivo se dirigieron a amedrentarlos en su labor como personas defensoras, en el sentido de limitar su intervención en el debate público y de restringir su labor de denuncia en el marco de la defensa y protección de los derechos humanos" (párrafo 965).

"[E]s factible, por vía de una interpretación evolutiva de [las] disposiciones [de la CADH] , desprender el reconocimiento de un derecho, propiamente dicho, a defender los derechos humanos . Este derecho autónomo puede resultar efectivamente vulnerado más allá de la particular conculcación de determinados derechos, como aquellos concernientes a la vida, a la integridad personal, a la libertad de expresión, a la libertad de reunión, a la libertad de asociación, a las garantías judiciales y a la protección judicial (listado al que cabe agregar el derecho de circulación y de residencia), y sin que necesariamente todos estos se declaren violados en un asunto concreto. Así las cosas, el contenido del derecho incorpora la posibilidad efectiva de ejercer libremente, sin limitaciones y sin riesgos de cualquier tipo, distintas actividades y labores dirigidas al impulso, vigilancia, promoción, divulgación, enseñanza, defensa, reclamo o protección de los derechos humanos y las libertades fundamentales universalmente reconocidas. En consecuencia, la imposición de limitaciones u obstáculos ilegítimos para desarrollar tales actividades de manera libre y segura por parte de las personas defensoras, en razón, precisamente, de su condición de tales y de las labores que realizan, puede conllevar la vulneración del derecho. Cabe aquí agregar que la calidad de persona defensora [...] está determinada por la naturaleza misma de las actividades desarrolladas, sin importar si se ejercen en forma ocasional o permanente, en el campo público o privado, de manera colectiva o individual, a nivel local, nacional o internacional, o si se contraen a específicos derechos civiles, políticos, económicos, sociales, culturales o ambientales, o se amplían al conjunto de estos" (párrafos 977 y 978).

8. PRUEBA INFORMÁTICA Y CADENA DE CUSTODIA

JURISPRUDENCIA NACIONAL

8.1. CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL FEDERAL, SALA I. "FISCAL S/ APELA DECLARACIÓN DE NULIDAD DE INFORME PERICIAL". CAUSA N° 46744. REGISTRO N° 458. 24/05/2012.

HECHOS

Un exfuncionario se encontraba siendo investigado por el delito de enriquecimiento ilícito. En el marco de ese proceso, se ordenó el allanamiento de la vivienda de su exasesor y la del hijo de éste, ambos involucrados en la investigación. El juzgado de primera instancia declaró la nulidad del punto II del auto de procesamiento respecto a las pericias practicadas por la División Apoyo Tecnológico de la Policía Federal Argentina sobre las computadoras secuestradas en el domicilio de la persona, así como también de la pericia que se había encomendado a los técnicos de la Universidad de Buenos Aires (UBA), junto con sus conclusiones, la información obtenida y la extracción de testimonios ordenadas a tal efecto. Contra esa decisión, el representante del Ministerio Público Fiscal presentó un recurso de apelación. Por su parte, ambas defensas —las del exasesor y la del exfuncionario—, sostuvieron que no habían sido notificados de la pericia informática de las computadoras secuestradas con el argumento de que se trataba de una operación sencilla y reproducible en el futuro. Y que, si bien fueron notificados de una nueva pericia, advertían, a partir del peritaje realizado por los expertos de la UBA, que el material recibido no había sido debidamente resguardado y que la cadena de custodia se encontraba comprometida. Por tanto, solicitaron que se anularan ambos peritajes, el primero por la omisión de practicar la notificación como establece la normativa procesal, y el segundo por la sospechosa contaminación de la evidencia que fuera advertida por los peritos de la UBA. La Cámara Federal en lo Criminal y Correccional se había pronunciado en este mismo incidente al respecto. En esa ocasión, anuló la resolución adoptada en primera instancia que rechazaba la nulidad impetrada por la defensa y ordenó practicar nuevas diligencias tendientes a esclarecer las circunstancias bajo las cuales se habían producido los peritajes practicados tanto por la División Apoyo Tecnológico de la Policía Federal como por la Facultad de Ciencias Exactas y Naturales de la UBA, para luego volver a decidir con el resultado de esas diligencias y en función del resto de las constancias de la causa vinculadas al planteo de nulidad de las pruebas obtenidas. Luego de realizarse las diligencias requeridas, el caso volvió a la Cámara.

DECISIÓN

La Sala I de la Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal, confirmó la resolución que anula los peritajes producidos por la Policía Federal y la UBA, y reenvió las actuaciones al Juzgado de Primera Instancia para que se prosiga sin esos elementos con la investigación del delito de enriquecimiento ilícito (jueces Ballestero y Farah).

ARGUMENTOS

1. Allanamiento. Notificación. Derecho de defensa. Derecho a la intimidad. Prueba. Derecho de exclusión.

"[O]tras reglas de garantía imponen la obligación de notificarlo de la realización de las medidas probatorias, sobre todo aquellas irreproducibles y de ofrecerle, en su caso, la posibilidad de proponer peritos, puntos sobre los cuales se ha fundado la protesta de la defensa en esta causa".

“Junto al control de la prueba, como derivado del derecho de defensa, también se encuentra involucrada la aplicación de otras reglas de garantías asociadas al derecho a la intimidad y a la inviolabilidad de la correspondencia epistolar y los papeles privados (´El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados…´ —art. 18 CN—), pues éstos sólo pueden ser intervenidos y utilizados como prueba de cargo cuando un juez lo autorice, por decisión fundada, a través de un procedimiento regularmente cumplido”.

“En aquella primera intervención de esta Cámara a la que antes se hizo alusión, se adelantó que el desconocimiento de esas reglas de garantía conducía a excluir la prueba y así fue como la encuesta se direccionó a superar el interrogante que contemplaba la posibilidad de que en autos se hubiese producido una actuación ilegítima o irregular en la incorporación de elementos de cargo a esta causa, en violación a las señaladas reglas”.

“Con el resultado de las diligencias ordenadas es que, entonces, han vuelto las actuaciones a decisión del Tribunal. Ellas, aunadas a las constancias del expediente obrante con anterioridad, abonan a nuestro entender el planteo de la defensa de los imputados”.

2. Derecho de defensa. Allanamiento. Orden judicial. Prueba informática. Nulidad. Informe pericial.

“[L]a orden de practicar la primera de las pericias, aquella que fue llevada a cabo por la División Apoyo Tecnológico de la Policía Federal [...], no fue notificada a las defensas de los imputados para que pudieran controlar su producción, pese a la expresa solicitud formulada por una de ellas de tener “…intervención… en todas las… pericias, inspecciones… que se lleven a cabo en la instrucción de la presente causa…´ [...], cuando, por el contrario, la lectura del expediente evidencia que la Fiscalía sí estaba avisada de dicho peritaje en curso [...]”.

“El art. 258 del CPPN (del capítulo correspondiente a la prueba pericial) dice que cuando un juez ordenare la realización de una pericia ´…notificará esta resolución al ministerio fiscal, a la parte querellante y a los defensores antes que se inicien las operaciones periciales, bajo pena de nulidad, a menos que haya suma urgencia o que la indagación sea extremadamente simple…´, disposición que resulta coherente con la manda general en materia de prueba contenida en el art. 201 del CPPN que establece que ´…antes de proceder a realizar alguno de los actos que menciona el artículo anterior [art. 200 ´…reconocimientos, reconstrucciones, pericias e inspecciones…que por su naturaleza y características se deban considerar definitivos e irreproducibles…´] …el juez dispondrá, bajo pena de nulidad, que sean notificados al ministerio fiscal, la parte querellante y los defensores… Solo en casos de suma urgencia se podrá proceder sin notificación…bajo pena de nulidad´”.

“Basta con dar lectura a los dos informes periciales cuestionados [...] como así también al producido luego por la Universidad Tecnológica Nacional [...], para descartar de plano y categóricamente que la peritación ordenada fuese una operación ´extremadamente simple´ de las que alude la norma citada (art. 258 CPPN), sobre todo si se tienen en cuenta las innumerables prevenciones señaladas por los mismos técnicos de la Universidad de Buenos Aires [...], así como la complejidad propia de las operaciones tendientes a la preservación de la evidencia, al uso de bloqueadores de escritura, a la búsqueda y recuperación de archivos informáticos, a su copiado, al uso de programas de recuperación de archivos eliminados o de observación de archivos ocultos, etc., etc., etc. Sobre este punto, que hace al núcleo del planteo de la defensa y que es relevante por lo antes expresado, los fiscales intervinientes nada han dicho”.

3. Allanamiento. Informe pericial. Orden judicial. Notificación. Secuestro. Plazo razonable.

“La ´urgencia´ alegada para realizar el peritaje sin notificación a las partes (puntualmente a quienes les fueron secuestradas las computadoras y que resultan también imputados en la causa junto a Ricardo Jaime, no así al Fiscal que sí estaba anoticiado) tampoco aparece explicada en el auto que ordenó la medida más allá de su mera invocación [...]. La mera transcripción de esa palabra no puede suplantar la indicación de los motivos en los que ella se debe asentar, pues está en juego un derecho que la ley acuerda a las defensas bajo expresa sanción de nulidad. Y a juzgar por las constancias del expediente inmediatamente posteriores al examen [...] el ´apuro´ originario se dirigió, antes que a estudiar el contenido y utilidad probatoria de los archivos electrónicos que halló la División Apoyo Tecnológico de la Policía Federal, a requerir-sin mayores explicaciones- un nuevo examen de las mismas computadoras con el objeto de buscar otros archivos electrónicos distintos [...], esta vez sí, curiosamente muy poco tiempo después de la primera, a la vista de las defensas. Qué fue lo que marcó la diferencia entre la primera y la segunda pericia para negar a las defensas su intervención en una y concederla en otra (con tan corto plazo de diferencia) no se sabe, pero del expediente surge con seguridad que no fue precisamente la urgencia (sobre todo si, además de lo ya dicho, se presta atención a que la UBA presentó su informe un año y medio después) y sobre esto, que hace al núcleo del planteo de las defensas, tampoco los fiscales intervinientes hicieron mención”.

“El fiscal, en procura de dar legal contención a lo aquí ocurrido, evoca la regla jurisprudencial sentada por la Cámara Nacional de Casación Penal según la cual la nulidad prevista en el Código Procesal sería de carácter relativo y puede considerarse subsanada si la defensa no la opone concretamente en tiempo y forma oportunos. No obstante, ella no encuentra aplicación en el caso desde que el planteo invalidante fue efectuado en esta causa dentro del plazo previsto en el art. 170, inc. 1°, del CPPN e, incluso, había mediado una petición formal de una de las defensas de participar ´…de todas las…pericias, inspecciones… que se lleven a cabo en la instrucción de la presente causa…´ antes de que la pericia en cuestión fuera llevada a cabo [...]”.

4. Informe pericial. Procedimiento policial. Prueba informática. Cadena de custodia. Derecho de exclusión.

“El carácter ´irreproducible´ de la primera de las pericias practicada (División Apoyo Tecnológico de la Policía Federal) si bien resultó acreditado con las comprobaciones efectuadas posteriormente sobre el modo como aquélla se llevó a cabo y sobre el resguardo (mejor dicho, no resguardo) de la evidencia por parte de dicha autoridad policial, ya se proclamaba —en esencia— desde mucho antes”.

“[L]a sola naturaleza de los elementos sometidos al examen pericial era ya suficiente alerta sobre la cautela y precauciones que correspondía adoptar, especialmente la observación de cada una de las solemnidades que debía revestir todo acto que los tuviera por objeto, tal como el máximo control en su desarrollo. Sin embargo, ninguna de esas circunstancias halló lugar aquí. Ello condujo, tal como los peritos de la UBA primero sugirieron y luego comprobaron, a la imposibilidad de aseverar que las computadoras secuestradas contuvieran —sin alteraciones, supresiones o adiciones— los mismos archivos que tenían registrados al momento de su secuestro y, por tanto, a tornar ilusoria la exacta reproducción de un estudio sobre ellas. La forma en que fue ordenado y conducido el peritaje hecho por la Policía Federal frustró así un segundo examen que, sin resquicio a duda, permitiera afirmar que los archivos consultados eran los mismos que se encontraban presentes en los ordenadores desde su incautación”.

“[C]abe recordar, en primer lugar, el informe producido por los técnicos de la Facultad de Ciencias Exactas y Naturales de la UBA [...], donde previnieron expresa y puntualmente acerca de las condiciones en que recibieron las computadoras y dieron cuenta de la imposibilidad de asegurar

—en vistas del modo como se llevó a cabo el estudio anterior— la cadena de custodia de la evidencia que habrían de analizar".

"En ese informe, a fs. 12.318/12.319, se da cuenta de lo siguiente: ´… 1) ENCABEZADO DEL INFORME… 2) INTRODUCCIÓN… 3) VALIDACIÓN Y VERIFICACIÓN DE LA CADENA DE CUSTODIA: A. [...] se solicitó al Juzgado la información correspondiente que avale el mantenimiento de la cadena de custodia del material secuestrado en donde se indicase fechas y horas en que dicho material fue obtenido por primera vez, y las fechas y horas en que el mismo fue utilizado en previa/s pericia/s si las hubiere, como así también los métodos informáticos utilizados para evitar la contaminación de la prueba. B. En la fecha 2 de febrero de 2010 al iniciarse la pericia, y en el momento de entrega del material a periciar, el Juzgado no proveyó la correspondiente documentación respaldatoria del mantenimiento de la cadena de custodia, indicando solamente en forma verbal que el material habría sido secuestrado el día 28/7/2009 y la pericia anterior fue finalizada el día 3/8/2009. C. La cadena de custodia se refiere a la fuerza o cualidad probatoria de la evidencia. Debe probarse (si fuese requerido por el juez o fiscal) que la evidencia presentada es realmente la misma evidencia recogida en la escena del crimen, o recuperada a través de algún testigo, entregada por la víctima, o por otros sujetos o adquirida originalmente de alguna otra forma. D. Para cumplir con este requisito debemos mantener un registro minucioso de la posesión y de la cadena de custodia de la evidencia. Este puede asegurarse mediante un sistema de recibos y registro minucioso. E. La cadena de custodia también implica que se mantendrá la evidencia en un lugar seguro, protegida de los elementos, que no se permitirá el acceso a la evidencia a personas que no están autorizadas. F. En el documento anexo denominado ´Descripción narrativa de la recepción de los efectos´ puede observarse que el material recibido del Juzgado no se encontraba adecuadamente protegido para su uso, ya que los puertos de alimentación eléctrica no estaban adecuadamente inhabilitados. G. Es una buena práctica de la profesión forense informática ´mantener y verificar la cadena de custodia´ para asegurar que todos los registros electrónicos originales no han sido alterados. H. En tal sentido y en virtud del estado del material a periciar que nos fuera entregado, no puede asegurarse que se haya mantenido la cadena de custodia. I. Consultado el juzgado sobre esta situación el día 9 de febrero en el momento de la devolución de la evidencia, el señor prosecretario […], manifestó conocer esta situación indicando que el juzgado igualmente deseaba obtener el resultado de la pericia…´" (el resaltado pertenece a la sentencia).

"Si las constancias de la causa obrantes al tiempo de la anterior resolución de esta Cámara ofrecían serias dudas sobre la legitimidad del modo en que se procedió, las diligencias practicadas con posterioridad conducen a nuestro juicio a excluir la prueba cuestionada. Por supuesto que son serias algunas de las objeciones que, al menos desde lo fáctico pero sólo desde lo fáctico-, oponen tanto el Fiscal de 1ª Instancia como el de Cámara para intentar salvar jurídicamente la validez de lo actuado, pero cada una de esas objeciones presenta su propia debilidad a poco que se las analiza en profundidad en base a las constancias de la causa y, en última instancia, ninguna de ellas salva el problema que se ha señalado más arriba: que según la ley, bajo pena de nulidad, la defensa tenía derecho a participar y controlar la producción de una pericia y fue excluida sin una justificación válida, y que luego se pretende utilizar en su contra una prueba que se dice hallada a través de un procedimiento cuya regularidad y eficacia se encuentran científicamente cuestionadas por no haberse preservado adecuadamente la evidencia, como también manda la ley".

5. Informe pericial. Procedimiento policial. Allanamiento. Cadena de custodia. Nulidad. Derecho de defensa.

"El análisis efectuado por el Fiscal de Cámara en los puntos IV a VI de su dictamen sostiene, en resumidas cuentas, que no es ´lógico´ pensar que al tiempo de practicarse la primera pericia (Policía Federal) se introdujeran en las computadoras secuestradas 7546 archivos para que luego

se omitiera señalar su hallazgo en el informe presentado al Juzgado. Sin embargo, frente a esa ´lógica´ del Sr. Fiscal de Cámara, las defensas oponen otra que desde el punto de vista ´lógico´ tiene igual grado de probabilidad: el primer estudio pericial fue realizado sin darles participación bajo el argumento falso de que se trataba de una operación extremadamente sencilla, urgente y repetible, y el sorpresivo hallazgo de los archivos electrónicos fue efectuado después, en un segundo peritaje, con su presencia pero sobre un material que no controlaron, habiéndose comprobado que no se habían adoptado los recaudos necesarios para asegurar la cadena de custodia de las computadoras, de suerte que los archivos electrónicos, que no estaban originalmente en ellas, habrían sido insertos luego del secuestro".

"La deducción que hacen los Fiscales acerca de que la evidencia obtenida de las computadoras por los peritos de la UBA no habría sufrido modificación alguna con posterioridad a su secuestro, que en apariencia se sostiene en la tarea del perito Gustavo PRESMAN en el estudio presentado en el marco de la causa n° 1219/09 del Juzgado n° 10 del fuero [...] es controvertible, por un lado, debido a que el propio perito PRESMAN fue categórico al reconocer que se había violado la cadena de custodia del material mientras estuvo a disposición de la División Apoyo Tecnológico de la Policía Federal [...] y, por otro, porque no asegura que los archivos electrónicos que luego hallaron los técnicos de la UBA hubieran estado originalmente en las computadoras, y esto último, que es precisamente aquello que habían denunciado las defensas y a lo que daba pábulo lo advertido por estos últimos profesionales (al señalar al deficiente forma de preservación de la evidencia), aparece ahora corroborado por la conclusión del nuevo peritaje practicado por el Licenciado en Sistemas Darío PICCIRILLI de la Universidad Tecnológica Nacional: ´no se puede afirmar inequívocamente que el contenido encontrado por los peritos de la Universidad de Buenos Aires era el mismo que al momento del secuestro´ [...]" (el resaltado pertenece a la sentencia).

"Y por si fuera poco, no ya sobre la preservación sino directamente sobre la autenticidad misma de la evidencia, se advierte el hallazgo de numerosos archivos creados con anterioridad al secuestro de las computadoras que aparecen modificados en el tiempo en que éstas estuvieron a disposición de la División Policial, o bien que fueron directamente creados en ese espacio de tiempo (ver punto F del informe pericial del Lic PICCIRILLI —Universidad Tecnológica Nacional— entre fs. 278 y 281 y el Anexo VII allí mencionado que tenemos a la vista)".

"La importancia de dicho hallazgo no es menor pues, de la lectura de dicho anexo, puede advertirse la existencia de archivos creados o modificados en aquel lapso que se refieren, en concreto, a algunas de las operaciones presuntamente delictivas que el Sr. Fiscal mencionó en la presentación efectuada a fs. 14.605 a partir de lo que había informado la UBA (vgr. ´…la compra de material rodante ferroviario a España y Portugal … reconcesión del Ferrocarril Belgrano Cargas… contrato de consultoría…´). Así, y más allá de cuál pudo haber sido la entidad o la extensión de la operatoria que los afectó, lo cierto es que este sólo aspecto —su modificación en un tiempo en el cual debieron permanecer imperturbables— impide a la magistratura acordarles algún valor probatorio [...]".

"A la par de las explicaciones que al respecto brindó el perito PICCIRILLI, no puede soslayarse que las advertencias de los profesionales de la UBA no se limitaron al punto señalado por el Fiscal. Por el contrario, como se dijo antes, el énfasis fue puesto en la falta de *´la documentación correspondiente que avale el mantenimiento de la cadena de custodia del material secuestrado en donde se indicase expresamente fechas y horas en que dicho material fue obtenido por primera vez y las fechas y horas en que el mismo fue utilizado en previa/s pericia/s si las hubiere, como así también los métodos informáticos utilizados para evitar la contaminación de la prueba´* [...]".

"[L]os peritos de la UBA no se refieren a la ausencia de fajado de los puertos de alimentación eléctrica a los que alude el Sr. Fiscal de Cámara como si sólo eso hubieran dicho, sino a las

circunstancias de lugar, tiempo y modo en que las computadoras secuestradas fueron manipuladas antes de que aquellos peritos las tuvieran a su disposición luego para estudio. Y entre esas circunstancias se encuentra, entre muchas otras que hablan de los rudimentarios métodos empleados por la Policía Federal, una de vital importancia: a diferencia de los peritos de la UBA, que emplearon sistemas bloqueadores de escritura de hardware (marca Tableau, tecnología SCSI, en todos los casos salvo en dos, que se empleó un Live CD de Linux denominado Knoppix) para ´…evitar que al acceder a los discos rígidos se inserte información espuria contaminando la evidencia...´ (conf. fs. 12.319 y 12.320) los peritos policiales no utilizaron ningún sistema de ese tipo (conf. pericia del Lic. PICCIRILLI de la UTN a fs. 267/284 y del Ing. PRESMAN a fs. 244/248)".

"De los rudimentarios métodos utilizados por la Policía Federal Argentina para la preservación de la evidencia es muestra también el hallazgo posterior de numerosos "archivos con fecha de modificación anterior a la fecha de creación" lo que resulta una "inconsistencia…inexplicable desde el punto de vista técnico" (ver informe del Lic. PICCIRILLI —Universidad Tecnológica Nacional— a fs. 281 y Anexo VIII al que remite)".

"[E]l propio perito PRESMAN, que citan los Sres. Fiscales, da cuenta en su informe en copia obrante a fs. 244/248 que ´…del análisis de los informes técnicos periciales existentes a fs. 1093 y 1098 del Expte. 12446/2008 del Juzgado Federal n° 7, se observa que en ninguno de ellos se describe con claridad las operaciones técnicas utilizadas, herramientas empleadas ni se hace mención a la utilización de bloqueadores de escritura. Tampoco se precisan las fechas en que se realizaron las operaciones…´, como así también que ´…las alteraciones a las que se refiere… serían producto de una negligencia operativa en las pericias informáticas efectuadas…".

"[D]ada la insistencia de los Sres. Fiscales en punto a que ninguno de los archivos creados o modificados durante el período en que las computadoras estuvieron a disposición de la División Apoyo Tecnológico de Policía Federal fueran archivos electrónicos correspondientes a mails o correos electrónicos, se advierte también de la lectura del Anexo VII de la pericia practicada por el Lic. PICCIRILLI de la Universidad Tecnológica Nacional, que ello no sería así, a poco que se repara en el listado correspondiente a la PC6– ACCEDIDOS – PARTICIÓN 1, y PC6 – CREADOS – PARTICIÓN 1, del citado Anexo VII, entre otros".

"No es que cándidamente se pretenda la más alta sofisticación en las prácticas de informática forense (´se tornan impracticables debido al cúmulo de causas a trabajar y al tiempo que demora aplicar estas recomendaciones en cada caso´ —ver declaración del Inspector Víctor Aquino a fs. 182—) desconociendo las limitaciones que pueden manifestarse en el orden local, sino simplemente que se preserve la prueba (conf. artículos 184, inc. 2°, y 261 primer párrafo, del CPPN) en lugar de contaminarla o poner en duda su contenido mediante operaciones desaprensivas sustraídas al control de las partes. Para mostrar el contraste entre ese proceder irregular y el actuar correcto y respetuoso del derecho de defensa, es forzosa la comparación con el imprevisto que aconteció al momento de practicarse el estudio de la UBA. Relató Rodolfo Baaer que al querer utilizar un dispositivo de hardware bloqueador —para tomar evidencia sin alterarla— se encontraron con que en uno de los casos ese dispositivo no soportaba la tecnología, por lo que, una vez avalado por los peritos de parte, se empleó un software para acceder (ver declaración testimonial a fs. 172/173)".

"[L]as prácticas llevadas adelante por la Policía Federal Argentina sobre el material secuestrado contaminaron la evidencia, convirtiendo lo que el juez instructor había considerado una ´operación pericial extremadamente simple´ y ´repetible´ en una medida irreproducible. De haberse dado la debida intervención a las defensas para que pudiesen presenciar y controlar aquellas prácticas, tal como sucedió con el estudio de la UBA, el inconveniente podría haberse superado, pero ello no sucedió. Se violó la regla de garantía contemplada expresamente por el

artículo 201 del código de rito —como derecho constitucional reglamentado— lo que cual conduce a la necesaria aplicación de la sanción que allí mismo también se establece (cfr. Maier, ob. cit., pág. 163)".

"Es por eso que se afirma que la peritación recién adquiere estado procesal cuando se cumplen todas las formalidades previstas por la ley (Clariá Olmedo, Jorge A. "Derecho Procesal Penal", Tomo Segundo, Marcos Lerner, 1984, Córdoba, pág. 401); y que ´cuando la ley impusiera alguna formalidad especial para su producción, relacionada con el derecho de defensa de las partes, la observancia de ella será también condición sine qua non para que la prueba que se obtenga pueda ser regularmente incorporada. Por ejemplo, si se tratara de un acto definitivo e irreproducible, se deberá notificar previamente a los defensores (arts. 201)…´ (Cafferata Nores, José I. ´La Prueba en el Derecho Penal´, Editorial Depalma, Buenos Aires, 1994, pág. 18)".

"Por más que pueda comprenderse la frustración evidenciada por los representantes del Ministerio Público Fiscal, de quienes es dable esperar igual esfuerzo y pasión por el resultado eficaz de las investigaciones de hechos de corrupción como por que éstas se lleven a cabo en correcta forma correcta (pues no se trata de terceros observadores sino de sujetos procesales especialmente comprometidos por imperio constitucional con la construcción, dentro del marco de la legalidad, de la verdad procesal entendida como meta del procedimiento), las restricciones impuestas a la actividad probatoria a través de las aludidas reglas de garantía carecería de sentido si la inobservancia de los preceptos no provocara la inadmisibilidad de incorporar al proceso los elementos de prueba obtenidos ilegítimamente, o bien excluirlos, si ya fueron incorporados (Maier, ob. cit., pág. 695). Es que ´…como resulta notorio, las razones de conveniencia —eventualmente, eficacia o celeridad— ceden —y deben ceder siempre— ante las garantías constitucionales en una estricta aplicación de éstas…´ (María Angélica Gelli, ´Constitución de la Nación Argentina, Comentada y Concordada´, Editorial La Ley, Buenos Aires, 2008, Tomo I, pág. 296)".

"Si la tarea realizada en primera instancia consolidó los indicios de violación de las reglas de garantía no es posible poner a cargo del titular de esas garantías la prueba fehaciente de su cumplimiento por parte del Estado y, mucho menos aún, justificar su inobservancia por el resultado buscado, incluso si se coincide con alguna de las ideas que con la elocuencia que lo caracteriza puso de resalto el Sr. Fiscal de Cámara en su dictamen obrante a fs. 343/352, desde que lo contrario importaría hacer prevalecer un principio de ´in dubio pro prueba´ contrario a la autolimitación que el Estado por ley se impuso. En el presente caso existían dos cosas que resultaba muy sencillo hacer y que se omitieron sin una justificación válida: una notificación a la defensa que manda la ley bajo pena de nulidad (artículos 200, 201 y 258, segundo párrafo, del CPPN) y la preservación adecuada de la evidencia que pretende usarse contra un individuo, exigida también por la ley (artículos. 184, inc. 2°, y 261 primer párrafo, del CPPN). Sólo es permitido arribar a la verdad por los medios y en la forma que la ley lo autoriza. Ese es el sentido de las reglas de garantía y si ellas no se han respetado, es misión ineludible de la magistratura, así declararlo (artículos166, 167, inc. 3°, y ccdts. del CPPN)".