GRAN SALA

ASUNTO BIG BROTHER WATCH Y OTROS C. REINO UNIDO

(*Demandas núms. 58170/13, 62322/14 y 24960/15*)

SENTENCIA

Artículo 8 • Vida privada • Cumplimiento del Convenio por el régimen de vigilancia secreta incluyendo la interceptación masiva de comunicaciones y el intercambio de inteligencia • Necesidad de desarrollar la jurisprudencia a la luz de las importantes diferencias entre la interceptación dirigida y la interceptación masiva • Test adaptado para examinar los regímenes de interceptación masiva a través de la evaluación global • Focalizar en las "salvaguardas de extremo a extremo" para valorar el creciente grado de intrusión en los derechos de privacidad en las diferentes etapas del proceso de interceptación masiva • Deficiencias fundamentales presentes en el régimen de interceptación masiva, por la falta de autorización independiente, por no incluir las categorías de selectores en la solicitud de una orden, y por la falta de autorización interna previa en el uso de selectores vinculados a una persona • Previsibilidad y salvaguardas suficientes en el régimen de recepción de inteligencia de servicios de inteligencia extranjeros • Régimen de obtención de datos relacionados con las comunicaciones por parte de proveedores de servicios de comunicaciones que no se llevan a cabo "de conformidad con la ley".

Artículo 10 • Libertad de expresión • Protección insuficiente del material periodístico confidencial sujeto a sistemas de vigilancia electrónica.

ESTRASBURGO

25 DE MAYO DE 2021

Esta sentencia es firme pero puede ser objeto de revisión editorial.

En el asunto Big Brother Watch y otros c. Reino Unido, el Tribunal Europeo de Derechos Humanos, reunido en Gran Sala compuesta por:

Robert Spano, *Presidente*,

Jon Fridrik Kjølbro,

Angelika Nußberger,

Paul Lemmens,

Yonko Grozev,

Vincent A. De Gaetano,

Paulo Pinto de Albuquerque,

Faris Vehabović,

Iulia Antoanella Motoc,

Carlo Ranzoni,

Mārtiņš Mits,

Gabriele Kucsko-Stadlmayer,

Marko Bošnjak,

Tim Eicke,

Darian Pavli,

Erik Wennerström,

Saadet Yüksel, *jueces*,

y Søren Prebensen, *Secretario Adjunto de la Gran Sala*,

Tras deliberar a puerta cerrada el 11 de julio de 2019, el 4 de septiembre de 2019 y el 17 de febrero de 2021 dicta la siguiente sentencia adoptada en la última de esas fechas:

PROCEDIMIENTO

1. El asunto se inició mediante tres demandas (núms. 58170/13, 62322/14 y 24960/15) interpuestas contra el Reino Unido de Gran Bretaña e Irlanda del Norte ante este Tribunal, en virtud del artículo 34 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales («el Convenio»), por las empresas, entidades benéficas, organizaciones e individuos enumerados en el anexo ("los demandantes") el 4 de septiembre de 2013, el 11 de septiembre de 2014 y 20 de mayo de 2015, respectivamente.

2. Los demandantes estuvieron representados por el Sr. Carey, de Deighton Pierce Glynn Abogados; la Sra. R. Curling, de Leigh Day and Co. Abogados; y la Sra. E.

Norton, de Liberty. El Gobierno del Reino Unido ("el Gobierno") estuvo representado por su Agente, el Sr. C. Wickremasinghe, del entonces Ministerio de Relaciones Exteriores y de la Mancomunidad de Naciones.

3. Los demandantes se quejaban del alcance y la magnitud de los programas de vigilancia electrónica utilizados por el Gobierno del Reino Unido.

4. Las demandas se notificaron al Gobierno el 7 de enero de 2014, el 5 de enero de 2015 y el 24 de noviembre de 2015, respectivamente. En el primer caso, se concedió la posibilidad de intervenir a Human Rights Watch, Access Now, Dutch Against dos Plasterk, Centro para la Democracia y la Tecnología, Red Europea de Instituciones Nacionales de Derechos Humanos y la Comisión de Igualdad y Derechos Humanos, la Fundación de Helsinki para los Derechos Humanos, la Comisión Internacional de Juristas, la Iniciativa de Justicia de la Sociedad Abierta, la Sociedad de Abogados de Inglaterra y Gales y Proyecto Moore. En el segundo caso, la posibilidad de intervenir fue concedida al Centro para la Democracia y la Tecnología, la Fundación de Helsinki para los Derechos Humanos, la Comisión Internacional de Juristas, la Unión Nacional de Periodistas y la Asociación de Abogados de los medios. En el tercer caso, se concedió la posibilidad de intervenir, de conformidad con el artículo 19 del Convenio, al Centro de Información sobre la Privacidad Electrónica y a la Comisión de Igualdad y de Derechos Humanos.

5. El 4 de julio de 2017, una Sala de la Sección Primera decidió acumular las demandas y celebrar una vista. Dicha vista pública tuvo lugar en la sede del Tribunal Europeo de Derechos Humanos, Estrasburgo, el 7 de noviembre de 2017. El 13 de septiembre de 2018, una Sala de la citada Sección, integrada por Linos-Alexandre Sicilianos, Kristina Pardalos, Aleš Pejchal, Ksenija Turković, Armen Harutyunyan, Pauliine Koskelo y Tim Eicke, jueces; y Abel Campos, Secretario de la Sección, dictaron sentencia. La Sala declaró inadmisibles, por unanimidad, las alegaciones formuladas por los demandantes en el tercero de los asuntos acumulados relativas al artículo 6 y al artículo 10, en la medida en que los demandantes se basaron en su condición de ONGs y en el artículo 14, y declaró admisibles el resto de las alegaciones planteadas por dichos demandantes. Por mayoría, se admitieron las alegaciones formuladas por los demandantes en el primero y el segundo de los asuntos acumulados. También por mayoría, se sostuvo que se había producido una violación de los artículos 8 y 10 del Convenio en relación con el régimen de la sección 8 (4) y el régimen del Capítulo II, y que no había habido violación del artículo 8 del Convenio en cuanto al régimen de intercambio de inteligencia. El voto particular parcialmente concurrente y parcialmente disidente del Magistrado Koskelo, junto con el Magistrado Turković, y el voto particular parcialmente disidente y parcialmente concurrente de los Magistrados Pardalos y Eicke, se acompañaron a la sentencia.

6. El 12 de diciembre de 2018 y el 11 de diciembre de 2018, respectivamente, los demandantes del primero y tercero de los asuntos acumulados solicitaron la remisión del caso a la Gran Sala de conformidad con el artículo 43 del Convenio. El 4 de febrero de 2019, el colegio de la Gran Sala accedió a dicha solicitud.

7. La composición de la Gran Sala se estableció de conformidad con las disposiciones del artículo 26 §§ 4 y 5 del Convenio y la Regla 24 del Reglamento del Tribunal.

8. Tanto los demandantes como el Gobierno presentaron alegaciones por escrito (Regla 59 §1) sobre la admisibilidad y el fondo del asunto.

9. El Presidente de la Gran Sala autorizó la intervención en el procedimiento escrito, de conformidad con el artículo 36 § 2 del Convenio y la Regla 44 § 3 del Reglamento, a los Gobiernos de Francia, Noruega y los Países Bajos, y al Relator Especial de las Naciones Unidas sobre la promoción del derecho a la libertad de opinión y expresión.

10. El 10 de julio de 2019 se celebró una vista pública en la sede del Tribunal Europeo de Derechos Humanos de Estrasburgo.

Comparecieron ante el Tribunal:

(a) por parte del Gobierno

Sr. C. WICKREMASINGHE, *Agente*;

Sr. J. EADIE Q.C. y

Sr. J. MITFORD, *Abogado*;

Sr. R. YARDLEY,

Sra. L. MORGAN,

Sr. H. MAWBY,

Sr. T. RUTHERFORD y

Sr. J. KEAY-BRIGHT, *Asesores*;

(b) por la parte demandante

Sr. B. JAFFEY Q.C.,

Sra. H. MOUNTFIELD Q.C.,

Sr. C. MCCARTHY,

Sr. R. MEHTA,

Sra. G. SARATHY Y

Sr. D. HEATON, *Abogado*;

Sr. D. CAREY Y

Sra. R. CURLING, *Consejeros*.

11. El Tribunal oyó los discursos del Sr. Eadie, el Sr. Jaffey y Sra. Mountfield, así como las respuestas a sus preguntas.

LOS HECHOS

I. ANTECEDENTES

12. Las tres demandas se presentaron tras las revelaciones de Edward Snowden sobre los programas de vigilancia electrónica utilizados por los servicios de inteligencia de los Estados Unidos de América y Reino Unido.

13. Los demandantes, que se enumeran en el Anexo, mantenían la creencia de que probablemente, debido a la naturaleza de sus actividades, sus comunicaciones electrónicas habían sido interceptadas por los servicios de inteligencia del Reino Unido; habían sido obtenidas por los servicios de inteligencia del Reino Unido después de ser interceptadas por gobiernos extranjeros; y / o habían sido obtenidas por las autoridades del Reino Unido a través de los proveedores de servicios de comunicaciones ("CSPs" – siglas en inglés-).

II. LOS SISTEMAS APLICABLES A LA VIGILANCIA SECRETA POR INTERNET.

14. Las comunicaciones por Internet se transmiten principalmente a través de cables de fibra óptica submarinos instalados por los CSPs. Cada cable puede llevar varios "portadores", y hay aproximadamente 100.000 de estos portadores acoplados a Internet. Una sola comunicación a través de Internet se divide en "paquetes" (unidades de datos) que pueden transmitirse por separado a través de múltiples portadores. Estos paquetes viajarán a través de una combinación de los caminos más rápidos y baratos. En consecuencia, algunos o todos los paquetes de cualquier comunicación particular enviada de una persona a otra, ya sea dentro del Reino Unido o fuera de sus fronteras, se puede enrutar a través de uno o más países si ese es el camino más óptimo para los CSPs involucrados.

A. Reino Unido.

1. Intercepción masiva.

15. Las revelaciones de Edward Snowden hechas en 2013 desvelaron que la Sede General de Comunicaciones del Gobierno ("GCHQ" – siglas en inglés-, uno de los servicios de inteligencia del Reino Unido) estaba ejecutando una operación, cuyo nombre en clave era "TEMPORA", en virtud de la cual accedió y almacenó enormes volúmenes de datos extraídos de los portadores. Las autoridades del Reino Unido ni confirmaron ni negaron la existencia de una operación con el nombre en clave de TEMPORA.

16. Sin embargo, según el Informe de marzo de 2015 del Comité de Inteligencia y Seguridad del Parlamento ("el informe del ISC" – ver párrafos 142 a 149 siguientes), la GCHQ estaba utilizando principalmente dos sistemas de procesamiento para la interceptación masiva de comunicaciones.

17. El primero de los dos sistemas de procesamiento mencionados en el informe del ISC estaba dirigido a un porcentaje muy pequeño de portadores. Como las comunicaciones fluían a través de portadores objetivos, el sistema comparaba el tráfico con una lista de "selectores simples". Éstos eran identificadores específicos (por ejemplo, una dirección de correo electrónico) en relación con un objetivo conocido. Cualquier comunicación que coincidiera con los selectores simples era recopilada; salvo que fuera descartada automáticamente. Luego, los analistas llevaban a cabo un "proceso de clasificación" en relación con las comunicaciones recopiladas para determinar cuáles eran las de mayor valor de inteligencia y, por lo tanto, debían abrirse y leerse. En la práctica, solo una proporción muy pequeña de las comunicaciones interceptadas a través de este proceso fueron abiertas y leídas por los analistas. Según el informe del ISC, la GCHQ no tenía capacidad para leer todas las comunicaciones.

18. El segundo sistema de procesamiento estaba destinado a un número aún más pequeño de portadores (un subconjunto de aquéllos a los que accedía por el proceso descrito en el párrafo anterior) que fueron deliberadamente seleccionados por ser aquéllos que de forma más probable interceptarían comunicaciones de interés para los servicios de inteligencia. Este segundo sistema tenía dos etapas: primero, la aplicación inicial de un conjunto de "reglas de procesamiento" diseñadas para desechar el material que era menos probable que fuera de valor; y, en segundo lugar, la aplicación de consultas complejas al material seleccionado con el fin de extraer el que probablemente tuviera un mayor valor de inteligencia. Dichas búsquedas generaban un índice y únicamente las comunicaciones previstas en dicho índice podían ser examinadas por los analistas. Todas las comunicaciones que no se encontraban en dicho índice tenían que ser descartadas.

19. El marco legal para la interceptación masiva de comunicaciones vigente en el momento en el que ocurrieron los hechos se establece con detalle en el apartado de "legislación nacional aplicable". En resumen, la sección 8 (4) de la Ley de Regulación de Poderes de Investigación de 2000 ("RIPA"- siglas en inglés - ver párrafo 72 siguiente) permitía al Secretario de Estado emitir una orden para la "interceptación de comunicaciones externas", y de conformidad con la sección 16 de la RIPA (véanse los párrafos 84 a 92 siguientes) el material interceptado no podía ser seleccionado para ser leído, visualizado o escuchado, "según un factor que es referible a un individuo que se conoce que está en ese momento en las Islas Británicas".

2. Intercambio de inteligencia.

20. El capítulo 12 del Código de Prácticas sobre la Interceptación de Comunicaciones ("el Código IC" - ver párrafo 116 siguiente) establecía las circunstancias en las que los servicios de inteligencia del Reino Unido podían solicitar inteligencia a los servicios de inteligencia extranjeros, y los procedimientos que debían seguirse para realizar tales solicitudes. El Capítulo 12 se añadió al Código IC después de que el Tribunal de Poderes de Investigación ("el IPT" – siglas en inglés-) ordenara a los servicios inteligencia que divulgaran sus disposiciones para el intercambio de inteligencia en el curso del procedimiento incoado por los demandantes en el tercero de los asuntos acumulados ("el procedimiento de Liberty" - véanse los párrafos 28 a 60 siguientes).

3. Obtención de los datos relacionados con las comunicaciones por parte de los CSPs.

21. El Capítulo II de la RIPA y Código de Prácticas sobre la Interceptación de Comunicaciones regulaban el proceso mediante el cual algunas autoridades públicas podían solicitar datos relativos a determinadas comunicaciones a los CSPs (véanse los párrafos 117 a 121 siguientes).

B. Estados Unidos

22. La Agencia de Seguridad Nacional ("NSA" – siglas en inglés-) reconoció la existencia de dos operaciones denominadas "PRISM" y "Upstream".

1. El programa PRISM.

23. PRISM era un programa mediante el cual el Gobierno de los Estados Unidos obtuvo material de inteligencia (como, por ejemplo, comunicaciones) de los Proveedores de

Servicios de Internet ("ISPs"- siglas en inglés-). El acceso a dicha información a través de PRISM era específico y dirigido (en contraposición a la amplia capacidad de la "minería de datos"). La administración de los Estados Unidos declaró que el programa estaba regulado por la Ley de Vigilancia de Inteligencia Extranjera ("FISA" – siglas en inglés-) y las solicitudes de acceso a material a través de PRISM tenían que ser aprobadas por el Tribunal de Vigilancia de Inteligencia Extranjera ("FISC"- siglas en inglés-).

24. Los documentos de la NSA filtrados por Edward Snowden pusieron de manifiesto que la GCHQ tuvo acceso a PRISM desde julio de 2010 y lo utilizó para generar informes de inteligencia. La GCHQ reconoció que obtuvo información de los Estados Unidos la cual se habían obtenido a través de PRISM.

2. El programa Upstream.

25. Según los documentos filtrados, el programa Upstream permitía la recopilación del contenido y de datos relacionados con las comunicaciones a través de fibra óptica, cables e infraestructuras propiedad de los CSPs de los Estados Unidos. Este programa daba acceso a un amplio catálogo de datos globales, en particular a los de ciudadanos no estadounidenses, que podían recopilarse, almacenarse y buscarse utilizando palabras clave (para más detalles, véanse los párrafos 261 a 264 siguientes).

III. PROCEDIMIENTOS INTERNOS EN EL PRIMERO Y SEGUNDO DE LOS ASUNTOS ACUMULADOS

26. Los demandantes en el primero de los asuntos acumulados (demanda núm. 58170/13) remitieron una reclamación previa al Gobierno el 3 de julio de 2013 exponiendo sus quejas y solicitando la declaración de que los artículos 1 y 3 de la Ley de Servicios de Inteligencia de 1994 ("ISA"- siglas en inglés -; véanse los párrafos 108 y 110 siguientes), la Sección 1 de la Ley de Servicios de Seguridad de 1989 ("SSA"- siglas en inglés-; véase el párrafo 106 siguiente) y la sección 8 de la RIPA (véase el párrafo 66 siguiente) eran incompatibles con el Convenio. En su respuesta de 26 de julio de 2013, el Gobierno declaró que en aplicación de la sección 65 (2) de la RIPA se excluían de la jurisdicción del Tribunal Superior las reclamaciones contra los servicios de inteligencia por vulneración de los derechos humanos, pero que las reclamaciones de los demandantes podían haberse planteado ante el IPT. El IPT era un Tribunal especializado creado por la RIPA para atender las alegaciones de los ciudadanos respecto de la interferencia ilícita en sus comunicaciones como resultado de una conducta amparada por esa ley, y estaba dotado de jurisdicción exclusiva para investigar cualquier reclamación relativa a que las comunicaciones de una persona hubieran sido interceptadas y, en caso de interceptación, examinar el poder para llevar a cabo dicha interceptación (véanse los párrafos 122 a 133 siguientes). Sin embargo, los demandantes no adoptaron más medidas.

27. Los demandantes en el segundo de los asuntos acumulados (demanda núm. 62322/14) no iniciaron ningún procedimiento interno ya que no consideraban que pudieran obtener una satisfacción efectiva frente a sus reclamaciones por el incumplimiento del Convenio.

IV. PROCEDIMIENTO INTERNO EN EL TERCERO DE LOS ASUNTOS ACUMULADOS.

28. Las diez organizaciones de derechos humanos que son demandantes en el tercero de los asuntos acumulados (demanda núm. 24960/15) presentaron individualmente una reclamación ante el IPT entre junio y diciembre de 2013 (en adelante "el procedimiento Liberty"). Alegaron que los servicios de inteligencia, el Secretario de Estado de Interior y el Secretario de Estado de Asuntos Exteriores habían actuado violando los artículos 8, 10, y 14 del Convenio al: (i) acceder o recibir comunicaciones y datos relacionados con las comunicaciones interceptados por los Estados Unidos bajo los programas PRISM y Upstream ("el asunto PRISM"); e (ii) interceptar, inspeccionar y retener comunicaciones y datos relacionados con las comunicaciones bajo el programa TEMPORA ("el asunto de la sección 8 (4)").

29. El 14 de febrero de 2014, el IPT acordó la acumulación de los diez asuntos anteriores. El Tribunal designó a un abogado (véase el párrafo 132 siguiente), cuya función era ayudar al IPT de cualquier forma que éste le indicara, incluyendo la representación en cuestiones en relación con las cuales no todas las partes pudieran estar representadas (por ejemplo, por razones de seguridad nacional).

30. En su respuesta a las reclamaciones de los demandantes, el Gobierno adoptó la postura de "ni confirmar ni negar", es decir, se negaron a confirmar o negar si las comunicaciones de los demandantes habían sido interceptadas. Por lo tanto, se acordó que el IPT determinaría la legalidad de la actuación sobre la base de la suposición de que la NSA había obtenido las comunicaciones y los datos relacionados con las comunicaciones de los demandantes a través de PRISM o Upstream y los había enviado a la GCHQ, donde habían sido retenidos, almacenados, analizados y compartidos; y que las comunicaciones y los datos relacionados con las comunicaciones de los demandantes habían sido interceptados por la GCHQ bajo el programa TEMPORA y habían sido retenidos, almacenados, analizados y compartidos. La cuestión era si, sobre estos hechos supuestos, la interceptación, retención, el almacenamiento e intercambio de datos era compatible con los artículos 8 y 10, analizados por sí solos y junto con el artículo 14 del Convenio.

A. La vista.

31. El IPT, compuesto por dos jueces del Tribunal Superior, un Juez de Circuito y dos abogados seniors, celebró una vista pública, durante cinco días, del 14 al 18 de julio de 2014. El Gobierno solicitó una vista a puerta cerrada adicional para permitir que el IPT pudiera valorar las disposiciones internas sobre el procesamiento del material interceptado de la GCHQ que no estaban publicadas -descritas durante la vista como disposiciones "por debajo de la línea de flotación"-. Los demandantes se opusieron, argumentando que la celebración de una vista a puerta cerrada no estaba justificada y que la falta de divulgación de las disposiciones era injusta.

32. La solicitud de una vista a puerta cerrada fue concedida de conformidad con la Regla 9 del Reglamento del IPT (véase el párrafo 129 siguiente). El 10 de septiembre 2014 tuvo lugar la vista a puerta cerrada en la que el IPT estaba "asistido por la plena, perceptiva y neutral participación... de los abogados del Tribunal", quienes desempeñaron las siguientes funciones: (i) identificación de documentos, partes de documentos o esencia de los mismos que debían divulgarse adecuadamente; (ii) hacer alegaciones a favor de la divulgación en interés de los demandantes y la justicia en

general; y (iii) asegurarse de que todos los argumentos relevantes (desde la perspectiva de los demandantes) sobre los hechos y la ley se sometieran al IPT.

33. En la vista a puerta cerrada, el IPT examinó las disposiciones internas ("por debajo de la línea de flotación") que regulaban las conductas y prácticas de los servicios de inteligencia. El 9 de octubre de 2014 el Tribunal notificó a los demandantes que consideraba que había algún material no publicado que podía ser divulgado. Explicó que había invitado al Gobierno a revelar dicho material y que el Gobierno había acordado hacerlo. En consecuencia, el material fue proporcionado a los demandantes en una nota ("la divulgación del 9 de octubre") y se invitó a las partes a presentar alegaciones al IPT sobre el citado material.

34. Los demandantes solicitaron información sobre el contexto y la fuente de divulgación, pero el IPT se negó a proporcionar más detalles. Los demandantes presentaron alegaciones por escrito sobre la divulgación.

35. Los demandados posteriormente modificaron y ampliaron el material revelado.

36. Tras las divulgaciones finales realizadas el 12 de noviembre de 2014, la divulgación del 9 de octubre establecía lo siguiente:

> "El Gobierno de EEUU ha reconocido públicamente que el programa Prism y el programa Upstream... permiten la obtención de comunicaciones de, desde o sobre selectores específicos asociados con personas no estadounidenses quienes se cree razonablemente que están ubicadas fuera de los Estados Unidos para obtener información de inteligencia extranjera. En la medida en que los Servicios de Inteligencia están autorizados por el Gobierno de los EEUU para atender solicitudes sobre el material obtenido a través del programa Prism (y / o ... a través del programa Upstream), dichas solicitudes solo pueden realizarse respecto a comunicaciones interceptadas que no han sido analizadas (y datos asociados a las comunicaciones) adquiridas de esta forma.
>
> 1. Los Servicios de Inteligencia solo pueden presentar una solicitud al Gobierno de un país o territorio fuera del Reino Unido sobre comunicaciones interceptadas no analizadas (y datos asociados a las comunicaciones), de otro modo que no sea de conformidad con un acuerdo internacional de asistencia judicial recíproca, si:
>
> > a. ha sido emitida la pertinente orden de interceptación en virtud de la [RIPA] por el Secretario de Estado, la asistencia del gobierno extranjero es necesaria para obtener las comunicaciones en cuestión porque no pueden obtenerse bajo la correspondiente orden de interceptación de la RIPA y es necesario y proporcionado para los servicios de inteligencia obtener esas comunicaciones; o
> >
> > b. la realización de la solicitud sobre las comunicaciones controvertidas, en ausencia de una orden de interceptación de la RIPA, no equivale a una elusión deliberada de la RIPA o que de otra manera contravenga el principio establecido en el asunto *Padfield c. Ministro de Agricultura, Pesca y Alimentació*n [1968] AC 997 [que un organismo público debe ejercer sus poderes discrecionales para promover (y no para eludir) la política y los objetivos de la legislación que le concedió esos poderes] (por ejemplo, porque técnicamente no es factible obtener las comunicaciones mediante la interceptación prevista en la RIPA), y es necesario y proporcionado para los Servicios de Inteligencia obtener esas comunicaciones. En estas circunstancias, la cuestión relativa a si la solicitud debe concederse será considerada y decidida personalmente por el Secretario de Estado. Cualquier solicitud de este tipo solo se hará en circunstancias excepcionales, lo que no ha ocurrido a la fecha de esta declaración.
>
> ...
>
> 2. Cuando los Servicios de Inteligencia reciban el contenido de comunicaciones interceptadas o los datos de dichas comunicaciones del gobierno de un país o territorio fuera del Reino Unido,

independientemente de si se han o no solicitado, de si el contenido ha sido analizado o no, o de si los datos relacionados con las comunicaciones están o no asociados con el contenido de las comunicaciones, el contenido de las comunicaciones y los datos están, de conformidad con las "disposiciones" internas, sujetos a las mismas reglas internas y salvaguardas que las mismas categorías de contenido o datos, cuando se obtienen directamente por los Servicios de Inteligencia como resultado de una interceptación llevada a cabo conforme a la RIPA.

3. Los Servicios de Inteligencia que reciban material interceptado sin analizar y datos relacionados con las comunicaciones interceptados bajo una orden de la sección 8 (4) cuentan con "disposiciones" internas que requieren la creación de un registro, explicando por qué se requiere el acceso al material interceptado no analizado, antes de que una persona autorizada pueda acceder a dicho material de conformidad con la sección 16 de la RIPA.

4. Las "disposiciones" internas de los servicios de inteligencia que reciben material interceptado no analizado y datos relacionados con las comunicaciones interceptados bajo una orden de la sección 8 (4) especifican (o requieren que se determine, en base a un sistema por sistema) períodos máximos de retención para las diferentes categorías de datos que reflejen la naturaleza y el grado de intrusión en los datos particulares en cuestión. Los períodos así especificados (o determinados) normalmente no superan los 2 años y, en ciertos casos, son significativamente más cortos (los informes de inteligencia que se basan en dichos datos se tratan como una categoría separada, y se conservan durante más tiempo). Los datos solo se pueden retener por un tiempo superior al período máximo de retención aplicable cuando se ha obtenido la autorización previa de un alto funcionario del Servicio de Inteligencia en cuestión sobre la base de que se ha evaluado que la conservación de los datos en cuestión continúa siendo necesaria y proporcionada (si se considera posteriormente que la retención continua de dichos datos, ya no cumple con el test de necesidad y proporcionalidad, dichos datos se eliminan). En la medida de lo posible, todos los períodos de retención se implementan mediante un proceso de eliminación automática que se activa una vez que se ha alcanzado el período máximo de retención aplicable para los datos en cuestión. Los períodos máximos de retención son supervisados y acordados con el Comisionado. En lo que respecta a los datos relacionados con las comunicaciones en particular, Sir Anthony May hizo una recomendación a los Servicios de Inteligencia que reciben material interceptado no analizado y datos relacionados con las comunicaciones interceptados bajo una orden de la sección 8 (4), y el Comisionado interino (Sir Paul Kennedy) recientemente se mostró conforme con la implementación de esa recomendación.

5. Las "disposiciones" internas de los Servicios de Inteligencia en el marco de la [Ley de Servicios de Seguridad de 1989], [la Ley de Servicios de Inteligencia de 1994] y los artículos 15 a 16 de la RIPA son revisados periódicamente para asegurar que permanecen actualizados y son efectivos. Además, los Servicios de Inteligencia tienen, en adelante, que considerar, durante el transcurso de dichas revisiones periódicas, si un mayor número de esas disposiciones internas podrían ser trasladadas de manera segura y útil al dominio público (por ejemplo, mediante su inclusión en un Código de prácticas)".

B. Primera sentencia del IPT de 5 de diciembre de 2014.

37. El IPT dictó su primera sentencia el 5 de diciembre de 2014. La sentencia abordó las disposiciones entonces vigentes para interceptar comunicaciones y la recepción de comunicaciones interceptadas por los servicios de inteligencia extranjeros.

1. El asunto PRISM.

38. El IPT aceptó que el asunto PRISM se encontraba vinculado al artículo 8 del Convenio, aunque a un "nivel inferior" que el considerado en el asunto *Weber y Saravia contra Alemania (dec.)*, núm. 54934/00, TEDH 2006 - XI. En consecuencia, las autoridades involucradas en el procesamiento de las comunicaciones recibidas por los servicios de inteligencia extranjeros debían cumplir con los requisitos del artículo 8, en particular en relación con su almacenamiento, intercambio, retención y destrucción. En opinión del IPT, siguiendo a *Bykov c. Rusia* [GC], núm. 4378/02, §§ 76 y 78, 10 de

marzo de 2009 y *Malone c. Reino Unido*, 2 de agosto de 1984, Serie A núm. 82, para que una interferencia sea considerada "de conformidad con la ley", no podía haber una discrecionalidad ilimitada en su ejecución; más bien, la naturaleza de las reglas tenía que ser clara y el ámbito de las normas tenía que ser, en la medida de lo posible, de dominio público. Sin embargo, consideró que, en el ámbito de la seguridad nacional, eran mucho menores los requerimientos de que fueran de dominio público y que el grado de previsibilidad exigido por el artículo 8 debía reducirse pues; de lo contrario, el fin de las medidas adoptadas para proteger la seguridad nacional estaría en riesgo (citando *Leander contra Suecia*, 26 de marzo de 1987, § 51, Serie A núm. 116).

39. El IPT continuó:

> "41. Consideramos que lo que se requiere es una señalización suficiente de la normativa o disposiciones en la medida en que no se divulguen ... Consideramos que en el campo del intercambio de inteligencia no es de esperar que las reglas deban estar contenidas en una ley (*Weber*) o incluso en un código (como se requería en virtud de la conclusión del Tribunal en *Liberty c. [Reino Unido*, núm. 58243/00, 1 de julio de 2008]). A nuestro juicio es suficiente que:
>
> i) Existan reglas o disposiciones apropiadas y su existencia sea de conocimiento público y este confirmada, con su contenido suficientemente señalizado, para proporcionar una indicación adecuada sobre ellas (según *Malone* ...).
>
> ii) Esten sujetas a la debida supervisión".

40. El IPT señaló que las disposiciones sobre el intercambio de información estaban previstas en el marco legal establecido en la Ley de Servicios de Seguridad 1989 (véanse los párrafos 105 a 106 siguientes) y la Ley de Servicios de Inteligencia 1994 (véanse los párrafos 107 a 110 siguientes). Además, se refirió a la declaración testifical realizada en el procedimiento Liberty antes mencionado por Charles Farr, Director General de la Oficina de Seguridad y Lucha contra el Terrorismo ("OSCT"- siglas en inglés-) del Ministerio de Interior, que explicó que el marco normativo establecido en esas leyes se sustentaba en detalladas orientaciones, incluyendo disposiciones para asegurar que los servicios solo obtenían la información necesaria para el correcto desempeño de sus funciones. Además, indicó que el personal recibía formación obligatoria sobre el marco legal y de políticas en los que operaban, incluyendo instrucciones sobre la necesidad de actuar en estricto cumplimiento de la Ley y la Guía. Finalmente, afirmó que los detalles completos de las disposiciones eran confidenciales, ya que no se podían publicar de forma segura sin menoscabar los intereses de seguridad nacional.

41. El IPT reconoció que, dado que las disposiciones no se habían hecho públicas, ni siquiera de forma resumida, no eran accesibles. Sin embargo, el IPT consideró significativo que las disposiciones estuvieran sujetas a la supervisión e investigación del Comité de Inteligencia y Seguridad del Parlamento ("el ISC" – sigas en inglés-) y la revisión independiente del Comisionado de Interceptación de Comunicaciones ("el Comisionado IC"). Además, el mismo estaba en condiciones de proporcionar supervisión, teniendo acceso a toda la información secreta, y podía aplazar la vista a puerta cerrada para evaluar si las disposiciones a las que se refería el Sr. Farr existían y tenían la capacidad de proporcionar protección individual ante injerencias arbitrarias.

42. Habiendo examinado las disposiciones "por debajo de la línea de flotación", el IPT mostró su conformidad con que la divulgación del 9 de octubre (modificada posteriormente, véase párrafos 33 y 36 anteriores) proporcionó un resumen claro y

preciso de esa parte de la prueba presentada en la vista a puerta cerrada, y que el resto de las evidencias presentadas en la vista a puerta cerrada eran demasiado sensibles para que se divulgaran sin causar un riesgo a la seguridad nacional o al principio de "ni confirmar ni negar". Además, se mostró conforme con que las condiciones previas para solicitar información al Gobierno de los Estados Unidos de América eran claras: tenía que existir una orden de la sección 8 (1), o una orden de la sección 8 (4) dentro de cuyo ámbito se encontraran las comunicaciones del objetivo propuesto, a la vez que, si se sabía que el individuo estaba en las Islas Británicas, una modificación de la sección 16 (3) (véase el párrafo 86 siguiente). Cualquier solicitud de interceptación de datos o comunicaciones a través de PRISM o Upstream estaba, por lo tanto, sujeta a la RIPA, a menos que se encontrara dentro del escenario totalmente excepcional descrito en 1 (b) relativo al material revelado después de la primera vista. Sin embargo, la solicitud prevista en el apartado 1 (b) nunca se había producido.

43. No obstante, el IPT identificó el siguiente "motivo de preocupación":

> "Si bien se da la circunstancia de que cualquier solicitud de, o recepción de, o interceptación de datos relacionados con las comunicaciones a través de Prism y / o Upstream normalmente está sujeta a las mismas salvaguardas que en un caso en el que se obtienen los datos de las comunicaciones directamente por los demandados, si hubiera una solicitud 1 (b), aunque dicha solicitud debe tramitarse ante la Secretaría de Estado, y cualquier material así obtenido debe ser tratado de conformidad con la RIPA, existe la posibilidad de que la protección de la sección 16 no se aplique. Como ya se ha indicado, en la práctica nunca se ha presentado ninguna solicitud 1 (b) y, por lo tanto, no ha habido problema hasta ahora. Sin embargo, consideramos que debe introducirse un procedimiento mediante el cual cualquier solicitud de este tipo, si se hace, cuando se refiera al Secretario de Estado, deba abordar las cuestiones de la sección 16 (3) ".

44. Sin embargo, en relación a esta salvedad, el IPT alcanzó las siguientes conclusiones:

> "(I) Habiendo considerado las disposiciones por debajo de la línea de flotación, como se describen en esta sentencia, mostramos nuestra conformidad con que existen disposiciones adecuadas para asegurar el cumplimiento del marco legal y de los artículos 8 y 10 del Convenio, en lo que respecta a la recepción de interceptación de Prism y / o Upstream.
>
> (ii) Por supuesto, esto no es suficiente en sí mismo, porque las disposiciones deben ser suficientemente accesibles al público. Mostramos nuestra conformidad con que están suficientemente señalizadas en virtud del marco legal al que nos hemos referido y las declaraciones del ISC y del Comisionado antes citadas, y como ahora, después de las dos vistas a puerta cerrada que hemos celebrado, divulgadas públicamente por los demandados y registradas en esta sentencia.
>
> (iii) Estas disposiciones están sujetas a supervisión.
>
> (iv) El alcance de la discrecionalidad conferida a los demandados para recibir y manejar material interceptado y datos relacionados con las comunicaciones y (materias sujetas a la sección 8 (4) referida a continuación) la forma de su ejercicio, son en consecuencia (en coherencia con *Bykov* – ver párrafo 37 anterior) accesibles con suficiente claridad para dar a la persona una adecuada protección contra las injerencias arbitrarias".

45. Finalmente, el IPT abordó un argumento planteado solo por Amnistía Internacional; a saber, que el Reino Unido tenía la obligación en virtud del artículo 8 del Convenio de evitar que Estados Unidos interceptara comunicaciones, incluida la obligación de no consentir tal interceptación recibiendo sus comunicaciones. Sin embargo, el IPT, citando *M. y otros contra Italia y Bulgaria*, núm. 40020/03, párrafo 127, 31 de julio de 2012, señaló que "los órganos del Convenio han manifestado reiteradamente que el Convenio no contiene un derecho que requiera a una Alta Parte Contratante a ejercer

una protección diplomática, o a adherirse a las reclamaciones de un demandante en virtud del derecho internacional, o de intervenir en su nombre ante las autoridades de otro Estado". Por tanto, el IPT rechazó este argumento.

2. La cuestión de la sección 8 (4)

46. El IPT formuló las cuatro cuestiones que debían resolverse para poder determinar si el régimen de la sección 8 (4) (que proporcionaba el marco legal para la interceptación masiva de comunicaciones externas) era compatible con el Convenio:

> "(1) ¿Es la dificultad de determinar la diferencia entre comunicaciones externas e internas... tal como para motivar que el régimen de la sección 8 (4) no se ajuste al artículo 8 (2)?
>
> (2) En la medida en que la sección 16 de la RIPA requiere como salvaguarda que la interferencia con el artículo 8 se lleve a cabo de conformidad con la ley, ¿es esto suficiente?
>
> (3) ¿El régimen, con o sin la aplicación de la sección 16, cumple suficientemente con los requisitos de Weber, en la medida en que son necesarios para cumplir con la ley?
>
> (4) ¿Es la sección 16 (2) indirectamente discriminatoria y contraria al artículo 14 del Convenio?, y, de ser así, ¿se puede justificar?"

47. En relación con la primera cuestión, los demandantes alegaron que tras el "cambio radical en la tecnología desde 2000", las comunicaciones eran ahora principalmente externas y, como resultado de ello, la distinción interna / externa de la sección 8 (4) ya no era "adecuada para su fin". Mientras que el IPT aceptó que los cambios en la tecnología habían sido sustanciales, y que era imposible diferenciar en la etapa de interceptación entre comunicaciones externas e internas, encontró que las diferencias en cuanto a la definición precisa de "comunicaciones externas" no se traducían *per se* la en la incompatibilidad del régimen de la sección 8 (4) con el artículo 8.2. En este sentido, consideró que la dificultad para distinguir entre comunicaciones "internas" y "externas" había existido desde la promulgación de la RIPA y los cambios en la tecnología no habían incrementado materialmente la cantidad o proporción de comunicaciones que no podían diferenciarse como externas o internas en el momento de la interceptación. En el peor de los casos, habían "acelerado el proceso de más cosas en el mundo en un verdadero análisis de lo que era externo e interno". En cualquier caso, la distinción sólo era relevante en la etapa de interceptación. El "trabajo pesado" era realizado por la sección 16 de la RIPA, que impedía que el material interceptado fuera seleccionado para ser leído, visualizado o escuchado "de acuerdo con un factor que es atribuible a un individuo que se conoce que está en ese momento en las Islas Británicas" (véanse los párrafos 84-92 siguientes). Además, todas las comunicaciones interceptadas en virtud de una orden de la sección 8 (4) solo podían ser consideradas para su examen por referencia a esa sección.

48. En relación con la segunda de las cuestiones, el IPT sostuvo que las salvaguardas previstas en la sección 16, que era aplicable únicamente al material interceptado y no a los datos relacionados con las comunicaciones, eran suficientes. Aunque concluyó que el criterio *Weber* se extendía también a los datos de comunicaciones, consideró que existía una protección o salvaguardas adecuadas en relación con la sección 15 de la RIPA (ver párrafos 77 a 82 siguientes). Además, en la medida en que la sección 16 ofrecía una mayor protección del contenido de las comunicaciones que de los datos relacionados con las comunicaciones, la diferencia estaba justificada y era proporcionada porque los datos de comunicaciones eran necesarios para identificar a las

personas cuyo material interceptado estaba protegido por la sección 16 (es decir, las personas que se conoce que se encuentran en el Islas Británicas).

49. Pasando a la tercera cuestión, el IPT concluyó que el régimen de la sección 8 (4) cumplía suficientemente con los criterios *Weber* (criterios establecidos en el asunto *Weber y Saravia*, antes citada, § 95; véanse también los párrafos 274 y 335 siguientes) y que, en todo caso, se actuó "conforme a la ley". Con respecto al primero y segundo de los requisitos, consideró que la referencia a la "seguridad nacional" era suficientemente clara (citando *Esbester c. Reino Unido* (dec.), núm. 18601/91, de 2 de abril de 1993 y *Kennedy c. Reino Unido*, núm. 26839/05, de 18 de mayo de 2010); la ausencia de un objetivo en la etapa de interceptación era aceptable e inevitable, como lo había sido en *Weber*; a primera vista, las disposiciones del párrafo 5.2 del Código IC, junto con los párrafos 2.4, 2.5, 5.3, 5.4, 5.5 y 5.6 (véase el párrafo 96 siguiente), fueron satisfactorias; no se requería que se incluyeran las palabras de búsqueda en la solicitud de una orden o en la propia orden, ya que esto innecesariamente socavaba y limitaba el funcionamiento de la orden y, en cualquier caso, podía ser completamente irreal; y no había ningún requisito para que la orden tuviera que ser autorizada judicialmente.

50. En relación con los criterios tercero, cuarto, quinto y sexto de *Weber*, el IPT tuvo en cuenta las salvaguardas de las secciones 15 y 16 de la RIPA, el Código IC y las disposiciones "por debajo de la línea de flotación". No consideró necesario que se publicasen los detalles precisos de todas las salvaguardas ni se previeran en normas o códigos de práctica. Particularmente en el campo de la seguridad nacional, las disposiciones administrativas no reveladas, que por definición pueden ser modificadas por el ejecutivo sin participación del Parlamento, pueden ser tenidas en cuenta, siempre que lo que se divulgue indique el alcance de la discrecionalidad y la forma de su ejercicio. Esto es especialmente así cuando, como en el caso que nos ocupa, el Código IC se refiere a las disposiciones, y establece un sistema de supervisión (conformado por el Comisionado IC, el propio IPT y el ISC) que asegura que las disposiciones estuvieran bajo revisión. El IPT se mostró satisfecho de que, como resultado de lo que había escuchado en la vista a puerta cerrada, no se había acumulado un gran banco de datos relacionados con las comunicaciones y existían las disposiciones adecuadas con respecto a la duración de la retención de los datos y su destrucción. Como en el asunto PRISM, el IPT consideró que las disposiciones de la sección 8 (4) estaban suficientemente señalizadas en las normas, en el Código IC, en los informes del Comisionado IC y, ahora, a su propia sentencia.

51. En cuanto a la cuarta y última cuestión, el IPT no se pronunció sobre si hubo discriminación indirecta por motivos de origen nacional como consecuencia de los diferentes regímenes aplicables a las personas ubicadas en las Islas Británicas y las ubicadas fuera de ellas, ya que consideró que cualquier discriminación indirecta estaba suficientemente justificada sobre la base de que era más difícil investigar las amenazas terroristas y criminales del exterior. Dado que el fin de acceder a las comunicaciones externas era principalmente obtener información relativa a aquéllos que se encontraban en el extranjero, la consecuencia de eliminar la distinción sería la necesidad de obtener un certificado según la sección 16 (3) de la RIPA (que excepcionalmente permitía el acceso a material relacionado con personas dentro de las Islas Británicas interceptado bajo una orden de la sección 8 (4) - ver el párrafo 86 siguiente-) en casi todos los casos, lo que radicalmente socavaba la eficacia del régimen de la sección 8 (4).

52. Por último, los demandantes alegaron que la protección otorgada por el artículo 10 del Convenio se aplica a las ONGs investigadas en la misma medida en que se aplica a los periodistas. Amnistía Internacional alegó inicialmente ante el IPT que era probable que no hubiera disposiciones adecuadas para el material protegido legalmente por el privilegio profesional, una reclamación que posteriormente "se separó" para ser tratada en el caso *Belhadj* (ver párrafos 99 a 101 siguientes), al que Amnistía Internacional se unió como demandante. No se planteó un argumento similar con respecto a la confidencialidad de las ONGs hasta el 17 de noviembre de 2014 (después de la primera y segunda vistas). Dado que el IPT consideró que este argumento podía haberse planteado en cualquier momento, a su juicio se había planteado "demasiado tarde" para ser tenido en cuenta en el procedimiento.

53. Con respecto a las demás reclamaciones relativas al artículo 10, el IPT señaló que no se planteaba un razonamiento separado del que se planteó con respecto al artículo 8. Si bien el IPT tuvo en cuenta el asunto *Sanoma Uitgevers B.V. contra los Países Bajos* [GC], núm. 38224/03, de 14 de septiembre de 2010, y destacó que el caso de los demandantes no se refería a la vigilancia selectiva de periodistas u organizaciones no gubernamentales. En cualquier caso, en su opinión, en el contexto de la vigilancia no dirigida a través de una orden de la sección 8 (4), sería "claramente imposible" anticipar una autorización judicial previa a la orden, limitada a aquello que pudiera llegar a impactar con el artículo 10. Aunque el IPT aceptó que podría surgir un problema en caso de que, en el transcurso del examen de los contenidos, surgiera alguna cuestión de confidencialidad periodística, había salvaguardas adicionales en el Código IC en relación con el tratamiento de tal material.

54. Tras la publicación de la sentencia, se invitó a las partes a hacer alegaciones sobre si, antes de las divulgaciones hechas al IPT, el régimen legal vigente con respecto a PRISM cumplía con los artículos 8 y 10, y sobre la proporcionalidad y licitud de cualquier presunta interceptación de sus comunicaciones. El IPT no consideró necesarias alegaciones adicionales sobre la proporcionalidad del régimen de la sección 8 (4) como un todo.

C. Segunda sentencia del IPT de 6 de febrero de 2015.

55. En su segunda sentencia de 6 de febrero de 2015, el IPT valoró si, antes de su sentencia de diciembre de 2014, las disposiciones sobre PRISM o Upstream violaron el artículo 8 y / o 10 del Convenio.

56. Estuvo de acuerdo en que solo tras la divulgación del 9 de octubre y sus modificaciones (véanse los párrafos 33 y 36 anteriores) el régimen era "conforme con la ley". El IPT consideró que, sin las divulgaciones realizadas, no habría habido una señalización adecuada, como se exigía en virtud de los artículos 8 y 10 del Convenio. Por lo tanto, declaró que antes de las divulgaciones:

> "23. ... [E] l régimen que rige la solicitud, recepción, almacenamiento y transmisión por las autoridades de Reino Unido de comunicaciones privadas de personas ubicadas en el Reino Unido, que han sido obtenidas por las autoridades de los Estados Unidos a través del sistema Prism y / o ... Upstream, infringió los artículos 8 o 10 del CEDH, pero ahora cumple con los mismos".

D. Tercera sentencia del IPT de 22 de junio de 2015 modificada por su carta de 1 de julio de 2015.

57. La tercera sentencia del IPT, publicada el 22 de junio de 2015, determinó que las comunicaciones de los demandantes obtenidas bajo PRISM o Upstream habían sido solicitadas, recibidas, almacenadas o transmitidas por las autoridades de Reino Unido en contravención de los artículos 8 y/o 10 del Convenio; y que las comunicaciones de los demandantes habían sido interceptadas, vistas, almacenadas o transmitidas por las autoridades del Reino Unido mediante un conjunto de conductas ilícitas o que contravienen los artículos 8 y / o 10.

58. El IPT no adoptó ninguna resolución en favor de ocho de los diez demandantes. De acuerdo con su práctica habitual por la que no se pronunciaba a favor de un demandante, no confirmó si sus comunicaciones habían sido o no interceptadas. Sin embargo, el IPT si adoptó resoluciones en relación con dos de los demandantes. La identidad de una de las organizaciones se anotó erróneamente en la sentencia y el error se corrigió mediante la carta del IPT de 1 de julio de 2015.

59. Con respecto a Amnistía Internacional, el IPT encontró que las comunicaciones por correo electrónico habían sido interceptadas de forma legal y proporcionada y que se había accedido a ellas de conformidad con la sección 8 (4) de la RIPA, pero que el límite de tiempo para la retención permitido bajo las políticas internas de la GCHQ se había sobrepasado y, por lo tanto, el material se había retenido durante más tiempo del permitido. Sin embargo, el IPT estaba convencido de que no se había accedido al material después de la expiración del plazo máximo de conservación pertinente y que la infracción podría caracterizarse como técnica. No obstante, apreció una infracción del artículo 8 y ordenó a la GCHQ que destruyera cualquiera de las comunicaciones que se habían retenido durante más tiempo del periodo permitido y a entregar una copia impresa de los documentos dentro de los siete días siguientes al Comisionado IC para que los conservara durante cinco años para el caso de que fueran necesarias en cualquier otro procedimiento legal. También se ordenó a la GCHQ que proporcionara un informe dentro del plazo de catorce días confirmando la destrucción de los documentos. No se le condenó al abono indemnización alguna.

60. Con respecto al Centro de Recursos Legales, el IPT concluyó que las comunicaciones de una dirección de correo electrónico asociada con el demandante habían sido interceptadas y seleccionadas para su examen según una orden de la sección 8 (4). Aunque mostró su conformidad con que la interceptación fue legal y proporcionada y la selección para el examen fue proporcionada, el IPT consideró que no se había seguido el procedimiento interno de selección. Por lo tanto, se había producido una violación de los derechos previstos en el artículo 8 respecto al Centro de Recursos Legales. Sin embargo, el IPT concluyó que no se hizo uso del material y que no se había conservado su registro por lo que el demandante no había sufrido detrimento, daño o perjuicio alguno. Por tanto, su resolución consistió en una satisfacción equitativa y no se otorgó compensación alguna por ello.

MARCO JURÍDICO APLICABLE Y COSTUMBRE.

I. DERECHO INTERNO APLICABLE

A. La interceptación de comunicaciones.

1. Autorizaciones: general

61. La sección 1 (1) de la RIPA 2000 (que ahora ha sido reemplazada por la Ley de Poderes de Investigación de 2016) ilegalizó la interceptación de cualquier comunicación en el curso de su transmisión por medio del servicio público de correo o un sistema público de telecomunicaciones, a menos que tuviera lugar de conformidad con una orden de la sección 5 ("orden de interceptación").

62. La sección 5 (2) permitía al Secretario de Estado autorizar una interceptación si consideraba que era necesaria por las razones expuestas en la sección 5 (3), a saber, en interés de la seguridad nacional, con el fin de prevenir o detectar delitos graves, o de salvaguardar el bienestar económico del Reino Unido (en la medida en que dichos intereses son también relevantes para los intereses de la seguridad nacional - véanse los párrafos 3.5 y 6.11 del Código IC y el párrafo 96 siguiente); y que la actuación autorizada por la orden fuera proporcionada en relación a lo que se pretenda lograr con la misma. Al evaluar la necesidad y la proporcionalidad, había que tener en cuenta si la información a la que se accedía en virtud de la orden podría haberse obtenido razonablemente por otros medios.

63. La sección 81 (2) (b) de la RIPA definió "delito grave" como un delito que cumple con uno de los siguientes criterios:

> "(a) que el delito o uno de los delitos que constituirían la conducta llevada a cabo es un delito por el cual una persona que ha cumplido veintiún años y no tiene condenas previas, se puede esperar razonablemente que sea condenado a prisión por un período de tres años o más;
>
> (b) que la conducta implique el uso de violencia, tenga como resultado una ganancia financiera sustancial o se trate de una conducta llevada a cabo por un gran número de personas en pos de un fin común".

64. La sección 81 (5) disponía:

> "A los efectos de esta Ley, se entenderá que la detección del delito incluye:
>
> (a) establecer por quién, con qué fin, por qué medios y, en general, en qué circunstancias se cometió cualquier delito; y
>
> b) la aprehensión de la persona por la que se cometió el delito;
>
> y toda referencia en esta Ley a la prevención o detección de delitos graves será interpretada en consecuencia ..."

65. La sección 6 disponía que, con respecto a los servicios de inteligencia, solo el Director General del MI5, el Jefe del MI6 y el Director de la GCHQ podían solicitar una orden de intercepción.

66. Había dos tipos de órdenes de interceptación a las que se referían las referidas secciones 5 y 6: una orden dirigida según lo dispuesto en la sección 8 (1), y una orden no dirigida según lo dispuesto en la sección 8 (4).

67. En virtud de lo establecido en la sección 9 de la RIPA, una orden emitida en interés de la seguridad nacional o para salvaguardar el bienestar económico de Reino Unido dejaba de tener validez al cabo de seis meses, y una orden emitida con el fin de detectar delitos graves dejaba de tener validez transcurridos tres meses. En cualquier momento antes de la finalización de esos plazos, el Secretario de Estado podía renovar la orden (por períodos de seis y tres meses, respectivamente) si consideraba que la orden seguía siendo necesaria por alguno de los motivos previstos en la sección 5 (3). El Secretario

de Estado debía cancelar una orden de interceptación si estaba convencido/a de que la orden ya no era necesaria por los motivos incluidos en la sección 5 (3).

68. De conformidad con la sección 5 (6), la conducta autorizada por una orden de interceptación tenía que incluir la interceptación de comunicaciones no identificadas por la orden si eran necesarias para llevar a cabo lo que estaba expresamente autorizado o requerido por la orden; y la obtención de datos de relacionados con las comunicaciones.

69. La sección 21 (4) definió los "datos relacionados con las comunicaciones" como:

> (a) cualquier dato del tráfico comprendido o adjunto a una comunicación (ya fuera por el remitente o de otro modo) para los fines de cualquier servicio postal o sistema de telecomunicaciones por medio del cual está siendo o puede ser transmitida
>
> (b) cualquier información que no incluya el contenido de una comunicación (distinta de cualquier información incluida en el párrafo (a)) y que trate del uso hecho por cualquier persona—
>
> > i. de cualquier servicio postal o de telecomunicaciones; o
> >
> > ii. en relación con la provisión o uso por parte de cualquier persona de cualquier servicio de telecomunicaciones, o de cualquier parte de un servicio de telecomunicaciones;
>
> (c) cualquier información que no esté incluida en los párrafos (a) o (b) que se mantenga u obtenga, en relación con las personas a las que presta el servicio, por una persona que proporciona un servicio postal o de telecomunicaciones".

70. El Código de prácticas sobre la interceptación de comunicaciones de marzo de 2015 se refirió a estas tres categorías como "datos del tráfico", "información de uso del servicio" e "información del abonado". La sección 21 (6) de la RIPA definió además los "datos del tráfico" como datos que identificaban a la persona, aparatos, ubicación o dirección hacia o desde la cual se enviaba/transmitía una comunicación, y la información de un archivo o programa informático al que se accede o que se ejecuta durante el envío o la recepción de una comunicación.

71. De acuerdo con la sección 20 de la RIPA, "datos relacionados con las comunicaciones", en relación con una comunicación interceptada en el curso de su transmisión por medio de un servicio postal o un sistema de telecomunicaciones, significaba "gran parte de cualquier dato de comunicaciones obtenido por, o en conexión con, la interceptación"; y relacionados "con la comunicación o con el remitente o el destinatario, o con el destinatario previsto, de la comunicación".

2. Autorizaciones: sección 8 (4)

(a) Autorización

72. La "interceptación masiva" de comunicaciones se llevaba a cabo de conformidad con una orden de la sección 8 (4). La Sección 8 (4) y (5) de la RIPA permitía al Secretario de Estado emitir una orden para "la interceptación de comunicaciones externas en el curso de su transmisión mediante un sistema de telecomunicaciones".

73. En el momento de emitir una orden de la sección 8 (4), al Secretario de Estado también se le solicitaba la emisión de un certificado en el que se estableciera una descripción del material interceptado que considerara necesario examinar, y declarando que consideraba que el examen de ese material era necesario por las razones expuestas

en la sección 5 (3) (es decir, que era necesario en interés de la seguridad nacional, con el fin de prevenir o detectar delitos graves, o para salvaguardar el bienestar económico de Reino Unido, en la medida en que esos intereses también sean relevantes para los intereses de seguridad nacional; ver s. 3.5 y 6.11 del Código IC en el párrafo 96 siguiente).

(b) Comunicaciones "externas"

74. La sección 20 definió la "comunicación externa" como "una comunicación enviada o recibida fuera de las Islas Británicas".

75. En el curso del proceso *Liberty*, Charles Farr, el Director General del OSCT, indicó que dos personas que se enviaban en el Reino Unido correos electrónicos entre sí estaban participando en una "comunicación interna" incluso si el servicio de correo electrónico estaba alojado en un servidor en los Estados Unidos de América; sin embargo, esa comunicación podría, no obstante, ser interceptada como un "captura incidental" de una orden dirigida a comunicaciones externas. De otra parte, una persona en el Reino Unido que se comunicara mediante un motor de búsqueda en el extranjero estaba participando en una comunicación externa, al igual que una persona en el Reino Unido que publicara un mensaje público (como un tweet o la actualización del estado de Facebook), a menos que todos los destinatarios de ese mensaje se encontraran en las Islas Británicas.

76. Presentadas pruebas al ISC en octubre de 2014, el Secretario de Estado para las Relaciones Exteriores y de la Mancomunidad de Naciones consideró que:

> "En el caso de un correo electrónico, si uno o ambos remitente o destinatario están en el extranjero, se trataría de una comunicación externa.
>
> En el caso de la navegación por Internet, si una persona lee el Washington Post en el sitio web, se ha "comunicado" con un servidor web ubicado en el extranjero, y por tanto se trata de una comunicación externa.
>
> En el caso de las redes sociales, si una persona publica algo en Facebook, dado que el servidor web tiene su base en el extranjero, se trataría de una comunicación externa.
>
> En el caso del almacenamiento en la nube (por ejemplo, archivos cargados en Dropbox), éstos serían tratados como comunicaciones externas, porque han sido enviados a un servidor web exterior."

3. Salvaguardas específicas en el marco de la RIPA

(a) Sección 15

77. De conformidad con la Sección 15 (1), era deber del Secretario de Estado asegurar, en relación con todas las órdenes de interceptación, que tales disposiciones estaban en vigor según lo considerara necesario para garantizar el cumplimiento de los requisitos de los incisos (2) y (3) en relación con la interceptación de material y cualquier dato relacionado con las comunicaciones; y, en el caso de órdenes en relación con las cuales se habían emitido los certificados de la sección 8 (4), que también se cumplieran los requisitos de la sección 16.

78. La sección 15 (2) disponía:

> "Se satisfacen los requisitos de esta subsección en relación con la interceptación de material y cualquier dato relacionado con las comunicaciones si cada uno de los siguientes requisitos:

a. el número de personas a las que se divulga el material o los datos o a quienes se les pone a disposición de otro modo,

b. la medida en que se divulga el material o los datos o se ponen a disposición de otro modo,

c. la medida en que se copia el material o los datos, y

d. el número de copias que se hacen,

se limita al mínimo necesario para los fines autorizados".

79. La sección 15 (3) disponía:

"Se satisfacen los requisitos de esta subsección en relación con la interceptación de material y cualquier dato relacionado con las comunicaciones si cada copia hecha de cualquiera de los materiales o los datos (si no se destruyen antes) se destruyen tan pronto como ya no exista cualquier motivo para retenerlos según sea necesario para cualquiera de los fines autorizados".

80. De conformidad con la sección 15 (4), era necesario para los fines autorizados si, y solo si, continuaba siendo, o era probable que llegara a ser necesario de conformidad con la sección 5 (3) de la Ley (es decir, fuese necesario en interés de la seguridad nacional, con el fin de prevenir o detectar delitos graves; con el fin de salvaguardar el bienestar económico del Reino Unido (en la medida en que esos intereses también sean relevantes para los intereses de la seguridad nacional - véanse los párrafos 3.5 y 6.11 del Código IC de acuerdo con el párrafo 96 siguiente); o con el fin de dar cumplimiento a las disposiciones de cualquier acuerdo internacional de asistencia mutua); era necesario para facilitar la realización de cualquiera de las funciones de interceptación del Secretario de Estado; era necesario para facilitar el desempeño de cualquier función del Comisionado IC o del IPT; era necesario para garantizar que una persona que lleva a cabo un proceso penal tuviese la información necesaria para determinar lo que requiere su deber de asegurar la equidad de la acusación; o era necesario para el cumplimiento de cualquier deber impuesto a cualquier persona bajo la legislación de registros públicos.

81. La sección 15 (5) requería que las disposiciones adoptadas para asegurar el cumplimiento de la sección 15 (2) incluyeran las disposiciones que el Secretario Estado considerara necesarias para asegurar que cada copia del material o de los datos que se hiciera se almacenara, durante el tiempo en el que se conservara, de forma segura.

82. De conformidad con la sección 15 (6), las disposiciones a las que se refiere la sección 15 (1) no eran necesarias para asegurar que se cumplían los requisitos de la sección 15 (2) y (3) en la medida en que estaban relacionadas con cualquier material interceptado o datos relacionados con las comunicaciones, o cualquier copia de dicho material o datos, cuya posesión se había entregado a las autoridades de un país o territorio fuera del Reino Unido. Sin embargo, se requerían tales disposiciones para asegurar, en el caso de cada una de esas órdenes, que la posesión del material y de los datos interceptados y de las copias del material o de los datos eran entregados a las autoridades de un país o territorio fuera del Reino Unido solo si se cumplían los requisitos de la sección 15 (7).

La sección 15 (7) disponía:

"Los requisitos de esta subsección se entienden cumplidos en el caso de una orden si el Secretario de Estado considera

a. que los requisitos correspondientes a las subsecciones (2) y (3) se aplicarán, en la medida (si corresponde) que el Secretario de Estado crea conveniente, en relación a cualquier material

> interceptado o a la posesión de datos relacionados en las comunicaciones, o a cualquier copia de los mismos, que se entreguen a las autoridades en cuestión; y
>
> b. que las restricciones en vigor impedirían, en la medida (si las hubiera) en que el Secretario de Estado crea conveniente, llevar a cabo cualquier actuación para los fines de o en conexión con cualquier procedimiento fuera del Reino Unido que daría lugar a una divulgación que, en virtud de la sección 17, no podría ser hecha en el Reino Unido".

83. La sección 17 de la RIPA disponía que, como regla general, no podía aducirse como prueba, realizarse una divulgación o llevarse a cabo cualquier otra actuación que revelara el contenido o los datos relacionados con las comunicaciones de una comunicación interceptada en relación con procedimientos legales.

(b) Sección 16

84. La sección 16 establece salvaguardas adicionales en relación con la interceptación de comunicaciones "externas" bajo la sección 8 (4). La sección 16 (1) requería que el material interceptado solo se pudiera leer, visualizar o escuchar por las personas a las que se les autorizaba en la orden y en la medida en que fuera certificado como material a examinar en la medida que fuera necesario conforme a lo dispuesto por la sección 5 (3) de la Ley; y entrara dentro de lo previsto en la sección 16 (2). La sección 20 definía "material interceptado" como el contenido de cualquier comunicación interceptada en virtud de una orden de interceptación.

85. La sección 16 (2) disponía:

> "Sujeto a las subsecciones (3) y (4), al material interceptado le es de aplicación esta subsección en la medida en que se seleccione para ser leído, visualizado o escuchado de otra manera que de acuerdo con un factor que–
>
> a. es referible a un individuo que se conoce que se encuentra por el momento en el Islas Británicas; y
>
> b. tiene como finalidad, o una de sus finalidades es, la identificación del material contenido en comunicaciones enviadas por él, o destinadas a él".

86. De conformidad con la sección 16 (3), el material interceptado se sometía a lo previsto en la sección 16 (2), sin perjuicio de que fuese seleccionado por referencia a uno de los factores mencionados en dicha subsección, si era certificado por el Secretario de Estado para los fines de la sección 8 (4) que el examen del material seleccionado de acuerdo con los factores atribuibles al individuo en cuestión, era necesario conforme a lo mencionado en la subsección 5 (3) de la Ley; y el material relacionado solo con comunicaciones enviadas durante el período especificado en el certificado que no era más largo que el máximo permitido.

87. El "máximo permitido" se definió en la sección 16 (3A) como sigue:

> (a) en el caso de material cuyo examen esté autorizado para los fines de la sección 8 (4) como necesario para el interés de la seguridad nacional, seis meses; y
>
> (b) en cualquier otro caso, tres meses".

88. De conformidad con la sección 16 (4), el material interceptado también se sometía a lo previsto en la sección 16 (2), incluso si se seleccionó por referencia a uno de los factores mencionados en esa subsección, si la persona a quien se le otorgó la orden consideraba, por motivos razonables, que las circunstancias concurrentes eran tales que

el material caía dentro de dicha subsección; o se cumplían las condiciones establecidas en la sección 16 (5) en relación con la selección del material.

89. La sección 16 (5) disponía:

> "Estas condiciones se cumplen en relación con la selección del material interceptado si:
>
> (a) la persona a quien se dirige la orden considera que se ha producido un cambio de circunstancias tan relevante como para, conforme a la subsección (4) (b), evitar que el material interceptado caiga dentro de la subsección (2);
>
> (b) desde que se concedió por primera vez, ha sido concedida una autorización por escrito para leer, visualizar o escuchar el material por un alto funcionario; y
>
> (c) la selección se realiza antes de que finalice el período permitido".

90. De conformidad con la sección 16 (5A), el "período permitido" significaba:

> "(a) en el caso de material cuyo examen esté autorizado para los fines previstos en la sección 8 (4) por ser necesario en interés de la seguridad nacional, el período termina al finalizar el quinto día hábil a contar desde el primer día que se puso a disposición como se menciona en la subsección (5) (a) de la persona a quien va dirigida la orden; y
>
> (b) en cualquier otro caso, el período finaliza al terminar el primer día hábil posterior al que se pusiera a disposición por primera vez a esa persona".

91. La sección 16 (6) explica que un "cambio relevante de circunstancias" significa que pareciera que el individuo en cuestión había entrado en las Islas Británicas; o que la creencia de que la persona a quien iba dirigida la orden se encontraba fuera de las Islas Británicas fuera equivocada.

92. Al entregar pruebas al ISC en octubre de 2014, el Secretario de Estado de Asuntos Exteriores y de la Mancomunidad de Naciones explicó que:

> "Cuando un analista selecciona comunicaciones que han sido interceptadas bajo una orden de las previstas en la sección 8 (4) para su examen, no importa la forma de comunicarse que utiliza el individuo, o si sus otras comunicaciones se almacenan en un servidor de correo o en una nube ubicada físicamente en el Reino Unido, en EEUU o en cualquier otro lugar (y en la práctica, el usuario individual de los servicios en la nube no sabe dónde se almacena). Si se sabe que se encuentra en las Islas Británicas, no está permitido buscar sus comunicaciones mediante el uso de su nombre, dirección de correo electrónico o cualquier otro identificador personal".

4. Código de prácticas sobre la interceptación de comunicaciones

93. La sección 71 de la RIPA disponía la obligación de adoptar por el Secretario de Estado códigos de prácticas en relación con el ejercicio y desempeño de sus poderes y obligaciones en virtud de la ley. Debían redactarse proyectos de códigos de prácticas para presentar ante el Parlamento y debían ser documentos públicos. Solo podían entrar en vigor de acuerdo con una orden del Secretario de Estado. El Secretario del Estado solo podía dictar una orden de ese tipo si se hubiera presentado un borrador ante el Parlamento y fuera aprobado por resolución de cada Cámara.

94. Según la sección 72 (1) de la RIPA, una persona que ejerza o actúe bajo cualquier poder o deber relacionado con la interceptación de comunicaciones tenía que atender a las disposiciones pertinentes de un código de prácticas. Las disposiciones de un código de prácticas podrían, en determinadas circunstancias, ser tenidas en cuenta por los tribunales conforme a lo dispuesto en la sección 72 (4) de la RIPA.

95. El Código IC se emitió de conformidad con la sección 71 de la RIPA. El Código IC vigente en el momento temporal que debemos enjuiciar se promulgó en 2016.

96. A los efectos que aquí nos conciernen, el Código IC disponía:

"3.2. Hay un número limitado de personas que pueden solicitar orden de interceptación, o en cuyo nombre se puede hacer una solicitud. Estas son:

- El Director General del Servicio de Seguridad.
- El Jefe del Servicio Secreto de Inteligencia.
- El Director de la Sede de Comunicaciones del Gobierno (GCHQ).
- El Director General de la Agencia Nacional contra el Crimen (la NCA lleva a cabo la interceptación en nombre de los organismos encargados de hacer cumplir la ley en Inglaterra y Gales).
- El Jefe de Policía del Servicio de Policía de Escocia.
- El Comisionado de la Policía de la Metrópoli (El Comando contra el Terrorismo de la Policía Metropolitana lleva a cabo la interceptación en nombre de las Unidades Antiterroristas, Unidades Especiales y algunas unidades especializadas de la policía en Inglaterra y Gales).
- El Jefe de Policía del Servicio de Policía de Irlanda del Norte.
- Los Comisionados de Hacienda y Aduanas de Su Majestad (HMRC).
- El Jefe de Inteligencia de Defensa.
- Una persona que, a los efectos de cualquier acuerdo de asistencia mutua internacional, sea la autoridad competente de un país o territorio fuera del Reino Unido.

3.3. Cualquier solicitud realizada en nombre de uno de los anteriores debe ser realizada por una persona que ocupe un cargo bajo la Corona.

3.4. Todas las órdenes de interceptación son emitidas por el Secretario de Estado. Incluso en los casos en los que se siga el procedimiento de urgencia, el Secretario de Estado autorizará personalmente la orden, aunque esté firmada por un alto funcionario.

Necesidad y proporcionalidad

3.5. Obtener una autorización conforme a la RIPA solo garantizará que la interceptación autorizada es una interferencia justificable con los derechos de una persona en virtud del artículo 8 (derecho al respeto de la vida privada y familiar) del Convenio Europeo de Derechos Humanos (CEDH) si es necesario y proporcionado que se lleve a cabo la interceptación. La RIPA garantiza lo anterior al requerir primero que el Secretario de Estado considere que la autorización es necesaria para uno o más de los siguientes motivos legales:

- En interés de la seguridad nacional;
- Para prevenir o detectar delitos graves;
- Para salvaguardar el bienestar económico del Reino Unido en la medida en que esos intereses también sean relevantes para los intereses de la seguridad nacional.

3.6. Estos fines se establecen en la sección 5 (3) de la RIPA. El Secretario de Estado debe asimismo considerar que la interceptación es proporcionada respecto a lo que se busca lograr mediante esa actuación. Cualquier evaluación de proporcionalidad implica sopesar la gravedad de la intromisión en la privacidad o propiedad del sujeto de la operación (o cualquier otra persona que pueda verse afectada) frente a la necesidad de la actividad de investigación, en términos operativos o de capacidad. La autorización no se considerará proporcionada si es excesiva en las circunstancias generales del caso. Cada acción autorizada debe conllevar un beneficio previsible para la investigación u operación y no debe ser desproporcionada o arbitraria. El hecho de que exista una amenaza potencial para la seguridad nacional (por ejemplo) puede que por sí solo no justifique las acciones más intrusivas. Ninguna interferencia será considerada proporcionada si la información que se pretende obtener pudiera, razonablemente, ser obtenida por otros medios menos intrusivos.

3. REGLAS GENERALES SOBRE INTERCEPCIÓN CON AUTORIZACIÓN

...

3.7. Por tanto, deben tenerse en cuenta los siguientes elementos en relación a la proporcionalidad:

- Equilibrar el tamaño y el alcance de la interferencia propuesta con lo que pretende obtenerse;
- Explicar cómo y por qué los métodos que se utilizarán causarán la menor intrusión posible sobre el sujeto y terceros;
- Considerar si la actividad se lleva a cabo de acuerdo con la legislación y de una manera razonable, habiendo considerado todas las alternativas razonables, para obtener el resultado necesario;
- Evidenciar, en la medida de lo posible, el uso de qué otros métodos se han considerado y no se han implementado o no se han empleado dado que se evalúan como insuficientes para cumplir los objetivos operativos sin aumentar el material de intercepción perseguido.

...

Duración de las órdenes de interceptación

3.18. Las órdenes de interceptación emitidas por delitos graves son válidas por un período de tres meses. Las órdenes de interceptación emitidas por motivos de seguridad nacional / bienestar económico del Reino Unido son válidas por un período inicial de seis meses. Una autorización expedida bajo el procedimiento de urgencia (por cualquier motivo) es válida por un plazo de cinco días hábiles desde su fecha de emisión a menos que sea renovada por el Secretario de Estado.

3.19. Una vez renovadas, las autorizaciones emitidas por delitos graves son válidas por un período adicional de tres meses. Las autorizaciones renovadas por motivos de seguridad nacional / bienestar económico del Reino Unido son válidas por un período adicional de seis meses. Estas fechas se computarán a partir de la fecha del documento de renovación.

3.20. Cuando se realicen modificaciones a una orden de interceptación, la fecha de expiración de la orden permanecerá inalterada. Sin embargo, cuando la modificación se tramite conforme al procedimiento de urgencia, la validez del documento de modificación expirará a los cinco días hábiles desde la fecha de emisión, a menos que se renueve por el procedimiento ordinario.

3.21. Cuando un cambio en las circunstancias lleva a la agencia interceptora a considerar que ya no es necesario, proporcionado o factible que una orden esté en vigor, la agencia debe hacer una recomendación al Secretario de Estado de que la cancele con efecto inmediato.

...

4. REGLAS ESPECIALES SOBRE LA INTERCEPCIÓN CON AUTORIZACIÓN.

Intrusión colateral

4.1. Se debe tomar en consideración cualquier interferencia con la privacidad de individuos que no son objeto de la interceptación prevista, especialmente cuando puede haber material involucrado de comunicaciones relacionadas con cuestiones religiosas, médicas, periodísticas o legalmente privilegiadas, o cuando pueden estar involucradas las comunicaciones entre un miembro del Parlamento y otra persona en asuntos de su circunscripción o comunicaciones entre un miembro del Parlamento y un denunciante. La solicitud de una orden de interceptación debe indicar si es probable que la interceptación dé lugar a un grado de violación colateral de la privacidad. La persona que solicita una orden de interceptación también debe considerar medidas, incluido el uso de sistemas automatizados, para reducir el alcance de la intrusión colateral. Cuando sea posible, la solicitud debe especificar esas medidas. Estas circunstancias y medidas se tendrán en cuenta por el Secretario de Estado al considerar la procedencia de una solicitud de una orden hecha bajo la sección 8 (1) de la RIPA. Si una operación de interceptación llegara al punto en que personas que no sean los sujetos previstos en la autorización se identifican como objetivos de la investigación por derecho propio, se debe considerar la posibilidad de solicitar una orden individual que cubra a esos individuos.

Información confidencial

4.2. También debe prestarse especial atención en los casos en los que el tema sobre el que se efectúa la interceptación podría ser razonablemente de un alto grado de privacidad, o cuando está

involucrada información confidencial. Esto incluye cuando las comunicaciones se relacionan con material legalmente privilegiado; cuando pueda estar involucrado material periodístico confidencial; cuando la interceptación pueda involucrar comunicaciones con un profesional médico o un Ministro de un culto religioso o con una persona relacionada con la salud o el bienestar espiritual; o en las comunicaciones entre un miembro del Parlamento y otra persona por cuestiones de circunscripción pueda estar involucrada.

4.3. El material periodístico confidencial incluye material adquirido o creado para fines de periodismo y sujeto al compromiso de confidencialidad, así como las comunicaciones que resulten para la adquisición de información con fines de periodismo y sujetas a tal fin. Ver también los párrafos 4.26. y 4.28 - 4.31 sobre las salvaguardas adicionales que deberían aplicarse con respecto al material periodístico confidencial.

...

Comunicaciones que involucran material periodístico confidencial, información personal confidencial y comunicaciones entre un miembro del Parlamento y otra persona en asuntos de su circunscripción.

4.26. También debe prestarse especial atención a la interceptación de comunicaciones que involucren material periodístico confidencial, información personal confidencial o comunicaciones entre un miembro del Parlamento y otra persona en asuntos de su circunscripción. El material periodístico confidencial se expone en párrafo 4.3. La información personal confidencial es información mantenida de forma confidencial concerniente a un individuo (ya sea vivo o muerto) que pueda ser identificado a partir de ella, y el material en cuestión se relaciona con su salud física o mental o asesoramiento espiritual. Dicha información puede incluir comunicaciones tanto orales como escritas. La información descrita anteriormente se mantiene de forma confidencial si se mantiene sujeta a un compromiso expreso o implícito de mantenerla en confidencialidad, o está sujeta a una restricción de su divulgación o a una obligación de confidencialidad contenida en la legislación vigente. Por ejemplo, la información personal confidencial puede incluir consultas entre un profesional de la salud y un paciente, o información de los registros médicos de un paciente.

...

4.28. Cuando la intención sea adquirir información personal confidencial, las razones deben estar claramente documentadas y la necesidad y proporcionalidad específicas de hacerlo, deben ser consideradas cuidadosamente. Si la adquisición de información personal confidencial es probable pero no intencionada, cualquier medida de mitigación posible debe ser considerada y, si no hay ninguna disponible, se debe considerar si se requieren disposiciones especiales de tratamiento dentro de la agencia interceptora.

4.29. El material que ha sido identificado como información confidencial debe ser retenido sólo cuando sea necesario y proporcionado hacerlo para uno o más de los fines autorizados establecidos en la sección 15 (4). Debe ser destruido de forma segura cuando su retención ya no sea necesaria para esos fines. Si se conserva dicha información, debe haber sistemas de gestión de la información adecuados para garantizar que la retención sigue siendo necesaria y proporcionada para los fines legalmente autorizados.

4.30. Cuando la información confidencial se retiene o se difunde a un organismo exterior, se deben tomar medidas razonables para marcar la información como confidencial. Cuando exista alguna duda sobre la licitud de la propuesta de manejo o difusión de información confidencial, se debe buscar el asesoramiento de un asesor legal dentro de la agencia de interceptación pertinente y antes de que tenga lugar cualquier divulgación adicional del material.

4.31. Cualquier caso en el que se retenga información confidencial debe notificarse al Comisionado IC tan pronto como sea razonablemente posible, conforme a lo acordado con el Comisionado. Cualquier material que se haya retenido debe ponerse a disposición del Comisionado si lo solicita.

4.32. Las salvaguardas establecidas en los párrafos 4.28 - 4.31 también se aplican a cualquier material previsto en la sección 8 (4) (véase el capítulo 6) que se seleccione para su examen y que constituya información confidencial.

...

6. GARANTÍAS DE INTERCEPCIÓN (SECCIÓN 8 (4))

6.1. Esta sección se aplica a la interceptación de comunicaciones externas mediante una orden que cumpla con la sección 8 (4) de la RIPA.

6.2. En contraste con la sección 8 (1), una orden de la sección 8 (4) no necesita nombrar o describir al sujeto de la interceptación o el conjunto de premisas en relación con las cuales se llevará a cabo la interceptación. Tampoco la sección 8 (4) impone un límite expreso al número de comunicaciones externas que pueden ser interceptadas. Por ejemplo, si se cumplen los requisitos de las secciones 8 (4) y (5), entonces, la interceptación de todas las comunicaciones transmitidas en una ruta o cable en particular, o llevadas a cabo por un CSP en particular, en principio, podrían ser legalmente autorizadas. Esto refleja el hecho de que la interceptación prevista en la sección 8 (4) es la capacidad de recopilación de inteligencia, mientras que la interceptación de la sección 8 (1) es principalmente una herramienta de investigación que se utiliza una vez que un sujeto en particular ha sido identificado para la interceptación.

6.3. La responsabilidad de la emisión de órdenes de interceptación bajo la sección 8 (4) de la RIPA recae en el Secretario de Estado. Cuando el Secretario de Estado emite una orden de este tipo, debe ir acompañada de un certificado. El certificado asegura que el proceso de selección se aplica al material interceptado de modo que solo el material descrito en el certificado esté disponible para el examen humano. Si el material interceptado no se puede seleccionar para ser leído, visualizado o escuchado con la debida atención a los criterios de proporcionalidad y los términos del certificado, entonces no se puede leer, visualizar o escuchar por nadie.

La interceptación de la Sección 8 (4) en la práctica

6.4. Una orden de la sección 8 (4) autoriza la interceptación de comunicaciones externas. Cuando una orden de la sección 8 (4) dé como resultado la adquisición de grandes volúmenes de comunicaciones, la agencia interceptora normalmente aplicará un proceso de filtrado para descartar automáticamente las comunicaciones que probablemente no tengan valor de inteligencia. Las personas autorizadas dentro de la agencia interceptora pueden entonces aplicar criterios de búsqueda para seleccionar las comunicaciones que probablemente tengan valor de inteligencia de acuerdo con los términos del certificado del Secretario de Estado. Antes de poder acceder a una comunicación en particular por una persona autorizada dentro de la agencia de interceptación, la persona debe proporcionar una explicación de por qué es necesario con base a una de las razones establecidas en el certificado que acompaña a la orden emitida por el Secretario de Estado, y de por qué es proporcionado en las circunstancias concretas. Este proceso está sujeto a auditoría interna y supervisión externa por parte del Comisionado de Intercepción de Comunicaciones. Cuando el Secretario de Estado tiene la certeza de que es necesario, puede autorizar la selección de comunicaciones de un individuo que se sabe que está en el Reino Unido. En ausencia de dicha autorización, una persona autorizada no debe seleccionar tales comunicaciones.

Definición de comunicaciones externas

6.5. Las comunicaciones externas son definidas por la RIPA como aquellas que se envían o reciben fuera de las Islas Británicas. Incluyen las que se envían y reciben fuera de las Islas Británicas, pasen o no por las Islas Británicas en el curso de su transmisión. No incluyen comunicaciones enviadas y recibidas en las Islas Británicas, incluso si pasan fuera de las Islas Británicas en ruta. Por ejemplo, un correo electrónico de una persona en Londres a una persona en Birmingham es una comunicación interna, no externa a los efectos de la sección 20 de la RIPA, se enrute o no a través de direcciones IP fuera de las Islas Británicas, porque el remitente y el destinatario previsto se encuentran dentro de las Islas Británicas.

Interceptación de comunicaciones no externas bajo una orden de la sección 8 (4)

6.6. La sección 5 (6) (a) de la RIPA aclara que la conducta autorizada por una orden de la sección 8 (4) puede, en principio, incluir la interceptación de comunicaciones que no sean comunicaciones externas en la medida en que sea necesario para interceptar las comunicaciones externas a las que se refiere la orden.

6.7. Al realizar una interceptación bajo una orden de la sección 8 (4), la agencia de interceptación debe utilizar sus conocimientos acerca de la forma en que las comunicaciones internacionales son enrutadas, combinadas con encuestas periódicas de enlaces de comunicaciones relevantes, para identificar aquellos portadores de comunicaciones individuales que tienen más probabilidades de contener comunicaciones externas que cumplan con la descripción del material certificado por el Secretario de Estado bajo la sección 8 (4). También debe realizar la interceptación de manera que limite la recopilación de comunicaciones no externas al nivel mínimo compatible con el objetivo de interceptar las comunicaciones externas deseadas.

Solicitud de una orden de la sección 8 (4)

6.8. La solicitud de la orden se realiza a la Secretaría de Estado. Las órdenes de interceptación, cuando se emiten, están dirigidas a la persona que presentó la solicitud. El fin de tal orden habitualmente reflejará una o más de las prioridades de inteligencia establecidas por el Consejo de Seguridad Nacional (NSC).

6.9. Antes de su presentación, cada solicitud está sujeta a una revisión dentro de la propia agencia desde la que se ha hecho la solicitud. Esto implica el escrutinio por parte de más de un funcionario, que ha de considerar si la solicitud es para uno de los fines incluidos en la sección 5 (3) de la RIPA y si la interceptación propuesta es necesaria y proporcionada.

6.10. Cada solicitud, una copia de la cual debe ser conservada por el solicitante, debe contener la siguiente información:

- Antecedentes de la operación en cuestión:
- Descripción de las comunicaciones a interceptar, detalles del (los) CSP (s) y una evaluación de la viabilidad de la operación cuando sea pertinente; y
- Descripción de la conducta a autorizar, la cual debe estar restringida a la interceptación de comunicaciones externas, o la conducta (incluida la interceptación de otras comunicaciones no identificadas específicamente por la orden conforme a lo previsto en la sección 5 (6) (a) de la RIPA) que es necesaria acometer con el fin de llevar a cabo lo autorizado o requerido por la orden, y la obtención de datos relacionados con las comunicaciones.
- El certificado que regulará el examen del material interceptado;
- La explicación de por qué la interceptación se considera necesaria para uno o más de los fines de la sección 5 (3);
- La consideración de por qué la conducta a ser autorizada por la orden es proporcionada a lo que se pretende lograr con esa conducta;
- Cuando una solicitud sea urgente, justificación de apoyo;
- La garantía de que el material interceptado será leído, visualizado o escuchado sólo en la medida en que esté certificado y cumpla las condiciones de secciones 16 (2) -16 (6) de la RIPA; y
- La garantía de que todo el material interceptado se manejará de acuerdo con las salvaguardas requeridas por las secciones 15 y 16 de la RIPA (ver párrafos 7.2 y 7.10 respectivamente).

Autorización de una orden de la sección 8 (4)

6.11. Antes de emitir una orden bajo la sección 8 (4), el Secretario de Estado debe considerar que la orden es necesaria:

- En interés de la seguridad nacional;
- Con el fin de prevenir o detectar delitos graves; o
- Con el fin de salvaguardar el bienestar económico del Reino Unido en la medida en que esos intereses también sean relevantes para los intereses de la seguridad nacional.

6.12. El poder de emitir una orden de interceptación con el fin de salvaguardar el bienestar económico del Reino Unido (según lo dispuesto en la sección 5 (3) (c) de la RIPA), sólo se ejercerá cuando el Secretario de Estado estime que las circunstancias son relevantes para los intereses de la seguridad nacional. El Secretario de Estado no emitirá una orden de la sección 5 (3) (c) si no existe un vínculo directo entre el bienestar económico del Reino Unido y la seguridad nacional. Cualquier

solicitud de orden bajo los motivos de la sección 5 (3) (c) debe identificar las circunstancias concurrentes que son relevantes para los intereses de la seguridad nacional.

6.13. El Secretario de Estado también debe considerar que la conducta autorizada por la orden es proporcionada a lo que busca lograr (sección 5 (2) (b)). En consideración de la necesidad y la proporcionalidad, el Secretario de Estado debe tener en cuenta si la información solicitada podría obtenerse razonablemente por otros medios (sección 5 (4)).

6.14. Cuando el Secretario de Estado emite una orden de este tipo, ésta debe estar acompañada de un certificado en el que el Secretario de Estado certifique que considera que el examen del material interceptado es necesario para uno o más de los fines de la sección 5 (3). La finalidad de este certificado previsto legalmente es asegurar que el proceso de selección se aplica al material interceptado de modo que solo el material descrito en el certificado está disponible para el examen humano. Cualquier certificado debe reflejar las "Prioridades para la recopilación de inteligencia" establecidas por el NSC para la orientación de las agencias de inteligencia. Por ejemplo, un certificado puede autorizar el examen de material que proporciona inteligencia sobre terrorismo (como se define en la Ley de Terrorismo de 2000) o de drogas sometidas a fiscalización (como se definen en la Ley de Uso Indebido de Drogas de 1971). El Comisionado de Interceptación de Comunicaciones debe revisar cualquier cambio en las descripciones del material especificado en un certificado.

6.15. El Secretario de Estado tiene el deber de cerciorarse de que las disposiciones estén vigentes para asegurarse de que solo el material que ha sido certificado como necesario para el examen para un fin de la sección 5 (3), y que cumpla con las condiciones establecidas en la sección 16 (2) en relación con la sección 16 (6), en la práctica, se lee, se visualiza o se escucha. El Comisionado de Interceptación de Comunicaciones tiene el deber de revisar la idoneidad de dichas disposiciones.

Autorización urgente de una orden de la sección 8 (4)

6.16. La RIPA prevé (sección 7 (l) (b)) los casos en los que una orden de interceptación sea requerida con urgencia, y el Secretario de Estado no esté disponible para firmar la orden. En estos casos, el Secretario de Estado también autorizará personalmente la interceptación, pero la orden será firmada por un alto funcionario, tras debatir del caso entre los funcionarios y la Secretaría de Estado. La RIPA restringe la emisión de órdenes por ese procedimiento a casos urgentes cuando el Secretario de Estado haya autorizado personal y expresamente la emisión de la orden (sección 7 (2) (a)), y requiere que la orden contenga una declaración a tal efecto (sección 7 (4) (a)).

6.17. Una orden emitida en virtud del procedimiento de urgencia tiene una validez de cinco días hábiles desde la fecha de su emisión a menos que sea renovada por el Secretario de Estado, en cuyo caso expira a los tres meses en el caso de delitos graves o seis meses en el caso de seguridad nacional o bienestar económico, al igual que las demás órdenes de las secciones 8 (4).

Formato de una orden de la sección 8 (4)

6.18. Cada orden está dirigida a la persona que presentó la solicitud. Una copia de la misma podrá ser entregada a los proveedores de servicios de comunicaciones que crea que podrán ayudar a implementar la interceptación. Los CSPs no recibirán normalmente una copia del certificado. La orden debe incluir lo siguiente:

- Una descripción de las comunicaciones que se van a interceptar;
- El número de referencia de la orden; y
- Datos de las personas que posteriormente podrán modificar el certificado aplicable a la orden en caso de urgencia (si está autorizado de acuerdo con sección 10 (7) de la RIPA).

Modificación de una orden y / o certificado de la sección 8 (4)

6.19. Las órdenes de interceptación y los certificados pueden modificarse según las disposiciones de la sección 10 de la RIPA. Una orden solo puede ser modificada por el Secretario de Estado o, en caso de urgencia, por un alto funcionario con autorización expresa del Secretario de Estado. En estos casos, la declaración sobre ese hecho debe ser refrendada en la modificación del instrumento, y la

modificación dejará de tener efecto después de cinco días hábiles desde de la fecha de su emisión a menos que esté respaldada por el Secretario de Estado.

6.20. Un certificado debe ser modificado por el Secretario de Estado, excepto en caso de urgencia, en el que un alto funcionario puede modificar un certificado siempre que ocupe un cargo en el que este expresamente autorizado por las disposiciones contenidas en el certificado para modificar el certificado en nombre del Secretario de Estado, o el Secretario de Estado haya autorizado expresamente la modificación y una declaración sobre este hecho se incluya en el instrumento modificativo. En este último caso, la modificación deja de tener efecto después de cinco días hábiles desde la fecha de su emisión a menos que sea avalada por el Secretario de Estado.

6.21. Cuando el Secretario de Estado considere que es necesario, un certificado puede modificarse para autorizar la selección de comunicaciones de un individuo que está en el Islas Británicas. La ubicación de una persona debe evaluarse utilizando toda la información disponible. Si no es posible determinar definitivamente dónde se encuentra ubicado el individuo utilizando esa información, se debe realizar una evaluación informada, de buena fe, en cuanto a la ubicación de la persona. Si se tienen sospechas fundadas que una persona se encuentra en el Reino Unido, se aplicarán las disposiciones establecidas en este párrafo.

Renovación de una orden de la sección 8 (4)

6.22. El Secretario de Estado puede renovar una orden en cualquier momento antes de su fecha de vencimiento. Las solicitudes de renovación se presentan a la Secretaría de Estado y deben contener una actualización de las cuestiones descritas en el párrafo 6.10 anterior. En particular, el solicitante debe proporcionar una evaluación del valor de la interceptación hasta la fecha y explicar por qué considera que la interceptación sigue siendo necesaria para uno o más de los fines previstos en la sección 5 (3), y por qué considera que la interceptación sigue siendo proporcionada.

6.23. Cuando el Secretario de Estado esté convencido de que la interceptación continúa cumpliendo con los requisitos de la RIPA, el Secretario de Estado puede renovar la orden. Cuando la orden se emite por motivo de un delito grave, la orden renovada es válida por tres meses más. Cuando se emite por motivos de seguridad nacional / bienestar económico, la orden renovada es válida por seis meses. Estas fechas van desde la fecha de firma del instrumento de renovación.

6.24. En aquellos casos en los que se haya solicitado la asistencia de un CSP, una copia del instrumento de renovación de la orden se enviará a todos aquellos a los que se les hubiera entregado una copia de la orden original, siempre que todavía estén asistiendo activamente. El instrumento de renovación incluirá el número de referencia de la orden que está siendo renovada en virtud de ese instrumento.

Cancelación de la orden

6.25. El Secretario de Estado debe cancelar una orden de interceptación si, en cualquier momento antes de su fecha de vencimiento, considera que la orden ya no es necesaria para los fines incluidos en la sección 5 (3) de la RIPA. Por tanto, las agencias interceptoras deben mantener sus órdenes bajo una revisión continua y deben notificar al Secretario de Estado si consideran que la interceptación ya no es necesaria. En la práctica, la responsabilidad de cancelar una orden será ejercida por un alto funcionario del departamento emisor en nombre de la Secretaría de Estado.

6.26. La cancelación estará dirigida a la persona a favor de quien se emitió la orden (la agencia interceptora). Una copia de la de cancelación debe enviarse a aquellos CSPs, si los hubiera, que hayan ejecutado la orden durante los doce meses anteriores.

Registros

6.27. El régimen de fiscalización permite al Comisionado de Interceptación de Comunicaciones inspeccionar la solicitud en la que se basa la orden del Secretario de Estado, y la agencia de interceptación puede ser requerida para que justifique el contenido. Cada agencia interceptora debe mantener lo siguiente para que esté disponible para su escrutinio por el Comisionado según lo requiera:

- Todas las solicitudes realizadas de órdenes que cumplan con la sección 8 (4), y solicitudes realizadas para la renovación de tales órdenes;
- Todas las órdenes y certificados, y copias de los instrumentos de renovación y modificación (si los hay);
- Cuando se rechace una solicitud, los motivos de denegación indicados por el Secretario de Estado;
- Las fechas en las que comenzó y terminó la interceptación.

6.28. También deben mantenerse registros de las disposiciones para asegurar que solo material que ha sido certificado para ser examinado conforme a un fin de los previstos en la sección 5 (3) y que cumpla las condiciones establecidas en la sección 16 (2) - 16 (6) de la RIPA de acuerdo con la sección 15 de la RIPA, es en la práctica, leído, visualizado o escuchado. Los registros de las disposiciones deben ser mantenidos de conformidad con los requisitos de la sección 15 (2) (minimización de copias y distribución del material interceptado) y la sección 15 (3) (destrucción del material interceptado) debe cumplirse. Para mayor detalle, consulte el capítulo sobre "Salvaguardas".

7. SALVAGUARDAS

7.1. Todo el material interceptado bajo una orden que cumpla con la sección 8 (1) o la sección 8 (4) de la RIPA y cualquier dato relacionado con las comunicaciones debe ser manejado de acuerdo con las salvaguardas que el Secretario de Estado ha aprobado de conformidad con el deber que le impone la RIPA. Estas salvaguardas están disponibles para el Comisionado de Interceptación de Comunicaciones, y deben cumplir los requisitos de la sección 15 de la RIPA que se establecen a continuación. Además, las salvaguardas de la sección 16 de la RIPA se aplican a las órdenes que dictadas bajo la sección 8 (4). El incumplimiento de estas salvaguardas debe ser reportado al Comisionado de Interceptación de Comunicaciones. Las agencias interceptoras deben mantener sus salvaguardas internas bajo revisión periódica para asegurar que permanezcan actualizadas y sean eficaces. Durante el curso de tales revisiones periódicas, las agencias deben considerar si un mayor número de sus disposiciones podrían ser puestas en el dominio público de manera segura y útil.

Las salvaguardas de la sección 15

7.2. La sección 15 de la RIPA requiere que la divulgación, copia y retención del material interceptado se limite al mínimo necesario para los fines autorizados. La sección 15 (4) de la RIPA establece que el material interceptado es necesario para dichos fines si:

- Sigue siendo, o es probable que sea, necesario para cualquiera de los fines establecidos en la sección 5 (3) - a saber, en interés de la seguridad nacional, con el fin de prevenir o detectar delitos graves, o con el fin, cuando consideradas las circunstancias por el Secretario de Estado le parezcan relevantes en interés de la seguridad nacional, de salvaguardar el bienestar económico del Reino Unido;
- Es necesario para facilitar el desempeño de las funciones del Secretario de Estado bajo el Capítulo I, Parte I de la RIPA;
- Es necesario para facilitar el desempeño de las funciones del Comisionado de Interceptación de Comunicaciones o del Tribunal;
- Es necesario para garantizar que una persona que lleva a cabo un proceso penal cuenta con la información necesaria para dar cumplimiento a su deber de garantizar la imparcialidad de la acusación; o
- Es necesario para el desempeño de cualquier deber impuesto por la legislación de registros públicos.

Difusión del material interceptado

7.3. El número de personas a las que se les revela el material interceptado, y el alcance de la divulgación, está limitado al mínimo necesario para los fines autorizados establecidos en la sección 15 (4) de la RIPA. Esta obligación se aplica tanto a la divulgación a personas adicionales dentro de una agencia, como a la divulgación fuera de la agencia. Dicha obligación implica la prohibición de divulgación a personas que no hayan sido debidamente evaluadas y también por el principio de necesidad de conocer: el material interceptado no debe ser divulgado a ninguna persona a menos que los deberes de esa persona, que deben estar relacionados con uno de los fines autorizados, sean tales

que necesite conocer el material interceptado para llevar a cabo esos deberes. De la misma manera, puede divulgarse solo una parte del material interceptado según las necesidades del destinatario. Por ejemplo, si un resumen del material interceptado fuera suficiente, no debe divulgarse más de eso.

7.4. Las obligaciones se aplican no solo al interceptor original, sino también a cualquiera a quien posteriormente se divulga el material interceptado. En algunos casos esto será logrado al requerir que este último obtenga el permiso del interceptor antes de divulgar el material interceptado. En otros, se aplican salvaguardas explícitas a los destinatarios.

7.5. Cuando el material interceptado se divulgue a las autoridades de un país o territorio fuera del Reino Unido, la agencia debe tomar medidas razonables para garantizar que las autoridades en cuestión tienen y mantendrán los procedimientos necesarios para salvaguardar el material interceptado, y para asegurarse de que sea revelado, copiado, distribuido y retenido sólo en la medida mínima necesaria. En particular, el material interceptado no debe ser revelado a las autoridades de un tercer país o territorio a menos que se haya acordado explícitamente con la agencia emisora, y debe ser devuelto a la agencia emisora o destruido de forma segura cuando ya no se necesite.

Proceso de copiado

7.6. El material interceptado solo puede copiarse en la extensión necesaria para los fines autorizados previstos en la sección 15 (4) de la RIPA. Se entiende por copias no solo las copias directas de todo el material interceptado, sino también los extractos y resúmenes que puedan identificarse como producto de una interceptación, y cualquier registro que se refiera a una interceptación que incluya las identidades de las personas para quienes o por quienes fue enviado el material interceptado. Las restricciones se implementan requiriendo un tratamiento especial de las copias, extractos y resúmenes que se realizan registrando su realización, distribución y destrucción.

Almacenamiento

7.7. El material interceptado y todas las copias, extractos y resúmenes del mismo, deben ser manipulados y almacenados de forma segura, a fin de minimizar el riesgo de pérdida o robo. El mismo debe ser almacenado de manera que sea inaccesible para las personas sin el nivel de evaluación requerido. El requisito de almacenar el producto interceptado de forma segura se aplica a todos los responsables de su manipulación, incluidos los CSPs. Los detalles relativos a lo que implicará tal requisito en la práctica para los CSPs se establecerán en las conversaciones que mantengan con el Gobierno antes de que se les entregue una Notificación de la Sección 12 (consulte el párrafo 3.13).

Destrucción

7.8. El material interceptado, y todas las copias, extractos y resúmenes que puedan ser identificados como productos de una interceptación, deben estar marcados para su eliminación y ser destruidos de forma segura tan pronto como sea posible una vez que ya no sean necesarios para ninguno de los fines autorizados. Si dicho material interceptado se retiene, debe revisarse en intervalos de tiempo apropiados para confirmar que la justificación para su retención sigue siendo válida bajo la sección 15 (3) de la RIPA.

7.9. Cuando una agencia de interceptación realiza la interceptación en virtud de una orden de la sección 8 (4) y recibe material interceptado no analizado y datos relacionados con las comunicaciones de la interceptación llevada a cabo bajo esa orden, la agencia debe especificar (o debe determinar con base a un sistema por sistema) los períodos máximos de retención para las diferentes categorías de datos que reflejen su naturaleza y el grado de intrusión. Los períodos especificados normalmente no deben ser superiores a los dos años, y deben acordarse con el Comisionado de Interceptación de Comunicaciones. Los datos solo pueden conservarse durante un tiempo superior a los períodos máximos de retención aplicables si se obtiene la autorización previa de un alto funcionario dentro de la agencia de interceptación sobre la base de que la retención de los datos continúa siendo necesaria y proporcionada. Si se considera más adelante que la retención continua de cualquiera de estos datos ya no cumple con los requisitos de necesidad y proporcionalidad, deben eliminarse. En la medida de lo posible, todos los períodos de retención deben ser implementados mediante un proceso de eliminación automática, que se active una vez que se ha alcanzado el período máximo de retención aplicable para los datos en cuestión.

Seguridad del Personal

7.10. Todas las personas que puedan tener acceso al material interceptado o necesiten acceder a informes en relación con él deben ser debidamente examinadas. Anualmente, los gerentes deben identificar cualquier indicio que aconseje que la evaluación de los antecedentes de algún miembro del personal deba ser reconsiderada. La evaluación de los antecedentes de cada miembro del personal también debe ser revisada periódicamente. Cuando sea necesario que un funcionario de una agencia divulgue material interceptado a otro, es responsabilidad del primero asegurarse de que el destinatario tiene la autorización necesaria.

Las salvaguardas de la sección 16

7.11. La sección 16 prevé salvaguardas adicionales en relación con el material obtenido bajo una orden de la sección 8 (4), requiriendo que las salvaguardas:

- Se aseguren de que el material interceptado sea leído, visto o escuchado por cualquier persona solo en la medida en que el material interceptado esté certificado; y
- Regulen el uso de selectores que se refieran a las comunicaciones de personas que se conoce que se encuentran en ese momento en las Islas Británicas.

7.12. Además, cualquier selección individual de material interceptado debe ser proporcionada teniendo en cuenta las circunstancias particulares (de conformidad con la sección 6 (1) de la Ley de Derechos Humanos de 1998).

7.13. El certificado asegura que se aplica un proceso de selección al material interceptado bajo una orden de la sección 8 (4) y que sólo el material descrito en el certificado está disponible para el examen humano (en el sentido de ser leído, visualizado o escuchado). Ningún funcionario tiene permitido acceder a datos que no sean los permitidos por el certificado.

7.14. Con carácter general, deben utilizarse sistemas automatizados, cuando sea técnicamente posible, para efectuar la selección de acuerdo con la sección 16 (1) de la RIPA. Como excepción, un certificado puede permitir el acceso al material interceptado por un número limitado de personas específicamente autorizadas sin haber sido procesado o filtrado por los sistemas automatizados. Dicho acceso solo podrá permitirse en la medida en que sea necesario para determinar si el material cae dentro de las categorías principales que se seleccionarán bajo el certificado, o para asegurarse de que la metodología que se utiliza permanece actualizada y es eficaz. Dicha verificación debe ser necesaria en sí misma por los motivos especificados en sección 5 (3) de la RIPA. Una vez cumplidas esas funciones, las copias que se hagan del material para esos fines deben ser destruidas de acuerdo con la sección 15 (3) de la RIPA. Este control por parte de los funcionarios deberá reducirse al mínimo posible; y, en su lugar, deberán utilizarse técnicas de selección automatizadas. La comprobación se mantendrá bajo la revisión del Comisionado de Interceptación de Comunicaciones durante sus inspecciones.

7.15. El material interceptado bajo una orden de la sección 8 (4) debe leerse, examinarse o escucharse solo por las personas autorizadas que reciban la formación regular obligatoria con respecto a las disposiciones de la RIPA y específicamente del funcionamiento de la sección 16 y los requisitos de necesidad y proporcionalidad. Estos requisitos y procedimientos deben establecerse en la guía interna proporcionada a todas las personas autorizadas y todas las personas autorizadas deben dirigir su atención específicamente a las salvaguardas legales. Todas las personas autorizadas deben ser debidamente evaluadas (ver párrafo 7.10 para mayor información).

7.16. Antes de que una persona autorizada pueda leer, ver o escuchar el material, se debe crear un registro que establezca de manera consistente por qué se requiere el acceso al material de conformidad con la sección 16 y el certificado correspondiente, y por qué dicho acceso es proporcionado. Salvo que se verifique el material o los sistemas automatizados conforme a lo descrito en el párrafo 7.14, el registro debe indicar, por referencia a factores específicos, el material al que se busca el acceso y los sistemas deben, en la medida en que posible, evitar el acceso al material a menos que se haya creado dicho registro. El registro debe incluir cualquier circunstancia que pueda dar lugar a una intrusión colateral en la privacidad, y cualquier medida tomada para reducir el alcance de tal intrusión colateral. Todos los registros deben conservarse para su posterior examen o auditoría.

7.17. El acceso al material descrito en el párrafo 7.15 debe limitarse a un período de tiempo definido, aunque el acceso pueda renovarse. Si se renueva el acceso, el registro debe actualizarse con el motivo de tal renovación. Los sistemas deben poder asegurar que, si no se realiza una solicitud de renovación dentro de ese período, entonces no se permitirá más el acceso. Cuando ya no se precisa el acceso al material, el motivo también debe indicarse en el registro.

7.18. Deben llevarse a cabo auditorías periódicas para garantizar que los requisitos establecidos en la sección 16 de la RIPA y el capítulo 3 de este Código se cumplen. Estas auditorías deben incluir verificaciones para garantizar que los registros que permitan el acceso al material que se van a leer, visualizar, o escuchar han sido correctamente compilados, y específicamente, que el material solicitado se circunscribe a las materias certificadas por la Secretaría de Estado. Cualquier error o deficiencia de procedimiento debe notificarse a la gerencia, y deben tomarse medidas para corregirlos. Cualquier deficiencia grave debe ser señalada a la alta dirección y cualquier incumplimiento de las salvaguardas (como se indica en el párrafo 7.1) debe ser reportado al Comisionado de Interceptación de Comunicaciones. Los informes de inteligencia generados por las personas autorizadas deben estar sujetos a una auditoría de control de calidad.

7.19. Para cumplir con los requisitos de la RIPA descritos en el párrafo 6.3 anterior, cuando un factor de selección se refiere a un individuo que se sabe que se encuentra en ese momento en las Islas Británicas, y tiene como fin o uno de sus fines es, la identificación de material contenido en las comunicaciones enviadas o destinadas a él o ella, la propuesta debe hacerse al Secretario de Estado o a un alto funcionario en caso de urgencia, dando una explicación de por qué es necesaria una modificación del certificado de la sección 8 (4) en relación con dicha persona conforme a un fin que se enmarque dentro de los previstos en la sección 5 (3) de la RIPA y es proporcionada en relación con cualquier conducta autorizada bajo la sección 8 (4) de la RIPA.

7.20. El Secretario de Estado debe asegurarse de que las salvaguardas estén en vigor antes de que pueda comenzar cualquier interceptación bajo una orden de la sección 8 (4). El Comisionado de Interceptación de Comunicaciones tiene el deber de revisar la idoneidad de las salvaguardas.

...

8. DIVULGACIÓN PARA GARANTIZAR LA EQUIDAD EN LOS PROCEDIMIENTOS PENALES

...

Exclusión de cuestiones sometidas a procedimientos legales

8.3. La regla general es que ni la posibilidad de interceptación, ni la interceptación de material en sí misma, juega ningún papel en los procedimientos legales. Esta regla se establece en la sección 17 de la RIPA, que excluye pruebas, cuestionamientos, afirmaciones o divulgaciones en procedimientos que probablemente revelen la existencia (o la ausencia) de una orden emitida bajo esta Ley (o la Ley de Interceptación de Comunicaciones de 1985). Esta regla significa que el material interceptado no puede ser utilizado ni por la acusación ni por la defensa. Esto preserva la "igualdad de armas", que es un requisito del artículo 6 del CEDH.

...

10. SUPERVISIÓN

10.1. La RIPA prevé un Comisionado de Interceptación de Comunicaciones, cuyo cometido es proporcionar una supervisión independiente del uso de los poderes contenidos en el régimen de interceptación regulado en el Capítulo I de la Parte I de la RIPA.

10.2. El Comisionado realizara inspecciones semestrales de cada una de las nueve agencias de interceptación. Los objetivos principales de las inspecciones son asegurar que el Comisionado tiene la información que requiere para el desempeño de sus funciones bajo la sección 57 de la RIPA y emitir su informe bajo la sección 58 de la RIPA. Esto incluye la inspección o consideración de:

- Los sistemas establecidos para la interceptación de comunicaciones;
- Los registros pertinentes mantenidos por la agencia interceptora;

- La licitud de la interceptación realizada; y
- Cualquier error y los sistemas diseñados para prevenirlos.

10.3. Cualquier persona que ejerza los poderes del Capítulo I de la Parte I de la RIPA debe informar al Comisionado de cualquier acción que se considere contraria a las disposiciones de la RIPA o cualquier cumplimiento inadecuado de las salvaguardas de la sección 15. Asimismo, debe cumplir con cualquier solicitud hecha por el Comisionado relativa a la remisión de cualquier información que el Comisionado le requiera con el fin de cumplir con sus funciones".

5. Declaración de Charles Farr.

97. En su testifical practicada en el proceso de Liberty (ver párrafo 40 anterior), Charles Farr indicó que, más allá de los detalles establecidos en la RIPA, en el Código IC de 2010 y en el proyecto de Código de CI de 2016 (que en ese momento se encontraba publicado para su consulta), los detalles exactos de las salvaguardas previstas en las secciones 15 y 16 se mantuvieron en secreto. Él había revisado personalmente las disposiciones y consideraba que no podían ser puestas en el dominio público de forma segura sin socavar la eficacia de los métodos de interceptación. Sin embargo, las disposiciones se pusieron a disposición del Comisionado IC a quien la RIPA le atribuía su revisión. Además, se pidió a cada agencia de interceptación que mantuviera un registro de las disposiciones en cuestión y cualquier incumplimiento tenía que ser comunicado al Comisionado IC.

6. Revisión de la estrategia de seguridad nacional y defensa estratégica y seguridad de 2015: Un Reino Unido seguro y próspero

98. En esta revisión, el Consejo de Seguridad Nacional ("NSC" -siglas en inglés-) declaró que sus prioridades durante los próximos cinco años serían:

"Abordar el terrorismo de frente en casa y en el extranjero de una manera dura e integral, contrarrestar el extremismo y desafiar las ideologías venenosas que lo alimentan. Nos convertiremos en el líder mundial en seguridad cibernética. Desalentaremos las amenazas al Estado. Responderemos a las crisis de forma rápida y eficaz y desarrollaremos resiliencia en el país y en el extranjero.

Contribuiremos a fortalecer el orden internacional basado en reglas y sus instituciones, alentando a la reforma para permitir una mayor participación de las potencias emergentes. Trabajaremos con nuestros socios para reducir los conflictos y promover la estabilidad, la buena gobernanza y los derechos humanos.

Promover nuestra prosperidad, ampliando nuestra relación económica con potencias emergentes como India y China, ayudando a construir la prosperidad global, invirtiendo en innovación y habilidades, y apoyando las exportaciones de seguridad y defensa del Reino Unido".

7. *Sentencia del IPT de 29 de marzo de 2015* en *Belhadj y otros c. Servicio de Seguridad, Servicio Secreto de Inteligencia, Sede de Comunicaciones del Gobierno, el Secretario de Estado de Interior y el Secretario de Estado de Relaciones Exteriores y de la Mancomunidad de Naciones, IPT / 13 / 132-9 / H e IPT / 14/86 / CH.*

99. Los demandantes en este caso alegaron la infracción de los artículos 6, 8 y 14 del Convenio como consecuencia de la presunta interceptación de sus comunicaciones legalmente privilegiadas. En la medida en que Amnistía Internacional, en el curso del procedimiento Liberty, planteó una reclamación acerca de la idoneidad de las disposiciones para la protección del material sujeto a privilegio profesional reconocido legalmente ("LPP"- siglas en inglés-), esas reclamaciones fueron "separadas" para ser

tratadas en este asunto, y Amnistía Internacional se unió como demandante (véase el párrafo 52 anterior).

100. En el curso del procedimiento, los demandados admitieron que, dado que no existía un sistema legal para tratar las LPP, desde enero de 2010 el régimen para la interceptación / obtención, análisis, uso, divulgación y destrucción de material legalmente privilegiado no se había realizado de conformidad con la ley conforme a lo establecido en el artículo 8.2 del Convenio y por lo tanto era ilegal. El Servicio de Seguridad y la GCHQ confirmaron que trabajarían en las próximas semanas para revisar sus políticas y procedimientos a la luz del proyecto del Código IC.

101. Posteriormente, el IPT celebró una vista a puerta cerrada, con la asistencia de los Abogados del Tribunal (véase el párrafo 132 siguiente), para valorar si los documentos o información relacionada con cualquier material legalmente privilegiado habían sido interceptados u obtenidos por los demandados. En su resolución de 29 de marzo de 2015, constató que los servicios de inteligencia solo habían obtenido dos documentos pertenecientes a los demandantes que contenían material sujeto a LPP, y no los revelaron ni remitieron al asesoramiento legal. Por lo tanto, concluyó que el demandante en cuestión no había sufrido perjuicio o daño alguno, y que la resolución proporcionó una satisfacción equitativa adecuada. Sin embargo, requirió al GCHQ para que presentara un compromiso de que las partes de los documentos que contenían material legalmente privilegiado serían destruidas o eliminadas; que se entregaría una copia de los documentos al Comisionado IC para ser retenidas durante cinco años; y que se presentaría un informe dentro del plazo de catorce días confirmando la destrucción y eliminación de los documentos.

102. Los proyectos de enmiendas tanto al Código de CI como al Código de prácticas de adquisición y divulgación de datos de comunicaciones fueron puestos a consulta y los Códigos que fueron adoptados como resultado en 2018 contenían secciones ampliadas sobre el acceso a la información privilegiada.

B. Intercambio de inteligencia

1. Acuerdo relativo a las comunicaciones en materia de inteligencia entre Gran Bretaña y EEUU.

103. El acuerdo relativo a las comunicaciones en materia de inteligencia entre Gran Bretaña y EEUU de 5 de marzo 1946 se aplicó a los acuerdos entre las autoridades de Gran Bretaña y de los Estados Unidos en relación con el intercambio de información de inteligencia relacionada con las comunicaciones "extranjeras", que eran definidas por referencia a países distintos de Estados Unidos, Reino Unido y de la Mancomunidad de Naciones. De conformidad con el acuerdo, las partes se comprometieron a intercambiar los resultados de una serie de operaciones de interceptación relativas a comunicaciones extranjeras.

2. Marco legal aplicable al funcionamiento de los servicios de inteligencia.

104. Hay tres servicios de inteligencia en el Reino Unido: el servicio de seguridad ("MI5"), el servicio secreto de inteligencia ("MI6") y la GCHQ.

(a) MI5

105. De conformidad con el artículo 2 de la Ley de Servicios de Seguridad de 1989 ("SSA" – siglas en inglés-), corresponde al Director General del MI5, designado por el Secretario de Estado del Ministerio del Interior, asegurarse de que existieran disposiciones que garantizaran que el MI5 no obtuviera información, excepto en la medida en que fuera necesario para el correcto desempeño de sus funciones o la divulgara excepto en la medida en que fuera necesario para ese fin o para el fin de la prevención o detección de delitos graves o para el fin de cualquier procedimiento penal.

106. De conformidad con el artículo 1 de la SSA, las funciones del MI5 eran las protección de la seguridad nacional y, en particular, su protección contra amenazas de espionaje, terrorismo y sabotaje, de las actividades de agentes de potencias extranjeras y de acciones destinadas a derrocar o socavar la democracia parlamentaria por medios políticos, industriales o violentos; salvaguardar el bienestar económico del Reino Unido contra amenazas planteadas por las acciones o intenciones de personas que se encuentran fuera de las Islas Británicas; y actuar en apoyo de las actividades de las fuerzas policiales, la Agencia Nacional del Crimen y otras agencias dedicadas a la prevención y detección de delitos graves.

(b) MI6

107. El artículo 2 de la Ley de Servicios de Inteligencia de 1994 ("ISA"– siglas en inglés-) dispone que las funciones del Jefe de Servicio del MI6, designado por el Secretario de Estado de Asuntos Exteriores y de la Mancomunidad de Naciones (como se denominaba en aquél entonces), incluían asegurarse de que existieran disposiciones que garantizaran que el MI6 no obtuviera información, excepto en la medida en que fuera necesario para el correcto desempeño de sus funciones o la divulgara excepto en la medida en que fuera necesario para ese fin o para el fin de la prevención o detección de delitos graves o para el fin de cualquier procedimiento penal.

108. De conformidad con el artículo 1 de la ISA, las funciones del MI6 eran: obtener y proporcionar información relacionada con las acciones o intenciones de personas fuera de las Islas Británicas; y realizar otras tareas relacionadas con las acciones o intenciones de dichas personas. Esas funciones solo podían ser ejercidas en interés de la seguridad nacional, con especial referencia a la defensa del Estado y las políticas de exterior; en interés del bienestar económico del Reino Unido; o en apoyo de la prevención o detección de delitos graves.

(c) GCHQ

109. El artículo 4 de la ISA disponía que era deber del Director de la GCHQ, designado por el Secretario de Estado de Relaciones Exteriores y Asuntos de la Mancomunidad de Naciones (como se denominaba en aquél entonces), asegurarse de que existieran disposiciones para garantizar que no se obtenía información excepto en la medida en que fuera necesaria para el correcto desempeño de sus funciones y que esa información no fuera revelada, excepto en la medida en que fuese necesario.

110. De conformidad con el artículo 3 de la ISA, una de las funciones de la GCHQ era monitorear o interferir mediante electromagnetismo, emisiones acústicas y otras emisiones cualquier equipo que produzca tales emisiones para obtener y proporcionar información derivada o relacionada con dichas emisiones o equipos y de material cifrado. Esta función sólo se podía ejercer en intereses de la seguridad nacional, con

especial referencia a la defensa del Estado y las políticas de exterior; en interés del bienestar económico del Reino Unido en relación con las acciones o intenciones de personas ajenas a las Islas Británicas; o en apoyo de la prevención o detección de delitos graves.

(d) La Ley de lucha contra el terrorismo de 2008.

111. El artículo 19 de la Ley contra el terrorismo de 2008 permitía la divulgación de información a cualquiera de los servicios de inteligencia para el ejercicio de cualquiera de las funciones que tenían atribuidas. La información obtenida por un servicio de inteligencia en relación con el ejercicio de alguna de sus funciones podía ser utilizada por dicho servicio en relación con el ejercicio de cualquier otra de sus funciones.

112. La información obtenida por el MI5 podía divulgarse para el adecuado desempeño de sus funciones, a los efectos de la prevención o detección de delitos graves, o con el fin de cualquier proceso penal. La información obtenida por el MI6 podía divulgarse para el adecuado desempeño de sus funciones, en interés de la seguridad nacional, con el fin de prevenir o detectar delitos graves, o con el fin de cualquier proceso penal. La información obtenida por la GCHQ podía ser divulgada para el adecuado desempeño de sus funciones o para el fin de cualquier proceso penal.

(e) La Ley de Protección de Datos de 1998 ("la DPA"- siglas en inglés-)

113. La DPA fue la norma que incorporó a la legislación del Reino Unido la Directiva 95/46 / CE sobre protección de datos personales. Cada uno de los servicios de inteligencia era un "controlador de datos" a los efectos de la DPA y, como tales, estaban obligados a cumplir la normativa - salvo exención por certificado ministerial- con los principios de protección de datos del Anexo I de la Parte 1, incluyendo:

> "(5) Los datos personales procesados para cualquier fin o fines no se conservarán más allá de lo que sea necesario para ese fin o fines..."
>
> y
>
> "(7) Se tomarán las medidas técnicas y organizativas apropiadas contra el procesamiento no autorizado o ilegal de datos personales y contra la pérdida accidental o destrucción o daño de datos personales".

(f) La Ley de Secretos Oficiales de 1989 ("la OSA" – siglas en inglés-)

114. Un miembro de los servicios de inteligencia cometería un delito bajo la sección 1 (1) de la OSA si él o ella revelara, sin autorización, cualquier información, documento u otro material relacionado con la seguridad o inteligencia que estuviera en su poder en virtud de su posición como miembro de ese servicio.

g) La Ley de derechos humanos de 1998 ("la HRA"- siglas en inglés-)

115. De conformidad con la sección 6 de la HRA, era ilegal que una autoridad pública llevara a cabo una actuación incompatible con un derecho reconocido en el Convenio.

3. Código de prácticas sobre la interceptación de las comunicaciones.

116. Con posterioridad al proceso Liberty, la información contenida en la divulgación de 9 de octubre (véanse los párrafos 33 y 36 anteriores) se incorporó al Código IC:

"12. REGLAS DE SOLICITUD Y MANEJO SIN ANÁLISIS DE COMUNICACIONES INTERCEPTADAS POR UN GOBIERNO EXTRANJERO

Ámbito de aplicación de este capítulo

12.1. Este capítulo se aplica a las agencias de interceptación que realizan la interceptación bajo una orden de la sección 8 (4).

Solicitudes de asistencia distintas a las que se lleven a cabo de conformidad con un acuerdo internacional de asistencia mutua.

12.2. Una agencia de interceptación solo puede hacer una solicitud al gobierno de un país o territorio fuera del Reino Unido de comunicaciones interceptadas no analizadas (y datos relacionados con las comunicaciones), de forma distinta a las que se lleven a cabo de conformidad con un acuerdo de asistencia mutua, si:

- La orden pertinente de interceptación bajo la RIPA ya ha sido emitida por el Secretario de Estado, la asistencia del gobierno extranjero es necesaria para obtener las comunicaciones particulares porque no se pueden obtener bajo la pertinente orden de interceptación de la RIPA y es necesario y proporcionado que la agencia interceptora obtenga esas comunicaciones; o
- La realización de la solicitud de las comunicaciones particulares en ausencia de la pertinente orden de interceptación de la RIPA no equivale a una la elusión de la RIPA o a frustrar de otro modo los objetivos de la RIPA (por ejemplo, porque no sea técnicamente factible obtener las comunicaciones vía interceptación de la RIPA), y es necesario y proporcionado que la agencia interceptora obtenga esas comunicaciones.

12.3. Una solicitud incluida en el segundo apartado del párrafo 12.2 solo podrá hacerse en circunstancias excepcionales y debe ser considerada y decidida por el Secretario de Estado personalmente.

12.4. A estos efectos, una "orden pertinente de interceptación de la RIPA" significa una de las siguientes: (i) una orden de la sección 8 (1) en relación con el sujeto en cuestión; (ii) una orden de la sección 8 (4) y un certificado adjunto que incluya una o más "descripciones del material interceptado" (en el sentido de la sección 8 (4) (b) de la RIPA) cubriendo las comunicaciones del sujeto, junto con una modificación conforme a lo previsto en la sección 16 (3) (para personas que se sabe que se encuentran dentro de las Islas Británicas); o (iii) una orden de la sección 8 (4) y un certificado adjunto que incluya una o más "descripciones de material interceptado" que cubren las comunicaciones del sujeto (por otras personas).

Salvaguardas aplicables al manejo sin análisis de comunicaciones interceptadas por un gobierno extranjero

12.5. Si una solicitud incluida en el segundo apartado del párrafo 12.2 es aprobada por el Secretario de Estado, salvo en relación con selectores específicos, cualquier comunicación obtenida no debe ser examinada por la agencia de interceptación de acuerdo con ningún factor como se menciona en la sección 16 (2) (a) y (b) de la RIPA a menos que el Secretario de Estado haya considerado y aprobado personalmente el examen de esas comunicaciones por referencia a tales factores.[1]

12.6. Cuando el contenido de las comunicaciones interceptadas o los datos relacionados con las comunicaciones obtenidas por las agencias interceptoras como se establece en el párrafo 12.2, o recibidos por ellas de otra manera por parte del gobierno de un país o territorio fuera del Reino Unido en circunstancias en las que el material se identifica a sí mismo como producto de una interceptación (excepto de conformidad con un acuerdo internacional de asistencia mutua), el

[1]Todas las demás solicitudes incluidas en el párrafo 12.2 (con o sin una orden pertinente de interceptación de la RIPA) se harán para el material hacía, desde o sobre selectores específicos (relacionados por lo tanto a un individuo o individuos específico/s). En estas circunstancias el Secretario de Estado ya habrá aprobado por lo tanto la solicitud para el/los individuo/s específico/a según lo establecido en el párrafo [sic.] 12.2.

contenido de las comunicaciones y los datos relacionados con las comunicaciones deben estar sujetos a las mismas normas y salvaguardas internas que se aplican a las mismas categorías de contenido o datos cuando son obtenidos directamente por las agencias interceptoras como resultado de la interceptación bajo la RIPA.

12.7. Todas las solicitudes en ausencia de una orden pertinente de interceptación de la RIPA al gobierno de un país o territorio fuera del Reino Unido de comunicaciones interceptadas no analizadas (y datos relacionados con las comunicaciones) serán notificadas al Comisionado de Interceptación de Comunicaciones".

C. Adquisición de los datos relacionados con las comunicaciones.

117. El capítulo II de la Parte 1 de la RIPA establece el marco en el que las autoridades públicas podrían adquirir datos de comunicaciones a través de proveedores de servicios de comunicaciones ("CSPs" – siglas en inglés-).

118. De conformidad con la sección 22, la autorización para la adquisición de los datos de comunicaciones a través de los CSPs era otorgada por la "persona designada", siendo ésta la persona que ocupe un cargo, rango o posición correspondiente al de una autoridad pública pertinente según lo dispuesto por una orden emitida por el Secretario de Estado. La persona designada podrá otorgar autorización al personal interno con la misma consideración de "autoridad pública pertinente" que él o ella y para "participar en conductas a las que se les aplica este Capítulo" (la autorización de la sección 22 (3)), o él o ella podría, mediante notificación al CSP, exigirle que divulgue los datos que ya están en su poder, u obtener y divulgar datos (el aviso de la sección 22 (4)). A los efectos de la sección 22 (3), las "autoridades públicas pertinentes" incluían a la policía, la Agencia Nacional contra el Crimen, el Servicio de Ingresos y Aduanas de su Majestad, cualquiera de los servicios de inteligencia y cualquier autoridad pública especificada como tal mediante una orden del Secretario de Estado.

119. La sección 22(2) disponía además que la persona designada solo podía otorgar una autorización bajo la sección 22 (3) o dar un aviso bajo la sección 22 (4) si creía que era necesario para uno de los siguientes fines:

"(a) en interés de la seguridad nacional;

(b) con el fin de prevenir o detectar delitos o de prevenir desórdenes;

(c) en interés del bienestar económico del Reino Unido;

(d) en interés de la seguridad pública;

(e) con el fin de proteger la salud pública;

(f) con el fin de calcular o cobrar cualquier impuesto, tasa, gravamen u otra imposición, contribución o cargo pagadero a un departamento gubernamental;

(g) con el fin, en caso de emergencia, de prevenir la muerte o lesiones o cualquier daño a la salud física o mental de una persona, o de mitigar cualquier lesión o daño a la salud física o mental de una persona; o

(h) para cualquier fin (no incluido en los párrafos (a) a (g)) que sea especificado mediante una orden del Secretario de Estado."

120. La persona designada debía también considerar que la obtención de los datos era proporcionada a lo que se pretendía lograr.

121. El Capítulo II de la RIPA se complementó con el Código de prácticas sobre la adquisición y divulgación de datos de comunicaciones, promulgado de conformidad con la sección 71 de la RIPA.

D. Práctica y procedimiento del IPT

1. RIPA

122. El IPT fue creado de conformidad con la sección 65 (1) de la RIPA para conocer sobre las alegaciones realizadas por ciudadanos relativas a injerencias indebidas en sus comunicaciones como resultado de una conducta de las reguladas por dicha ley. Tenía competencias para investigar cualquier reclamación sobre si se habían interceptado las comunicaciones de una persona y, cuando se había producido la interceptación, para examinar la legitimidad de tal interceptación.

123. Los nombramientos de los miembros del IPT fueron esencialmente de naturaleza judicial, pero se distinguía entre ellos dependiendo de si el candidato propuesto era un miembro en activo del poder judicial sénior de Inglaterra y Gales, Escocia o Irlanda del Norte (referido como un "miembro judicial") o de si se trataba de un "miembro no judicial". Un miembro no judicial podía ser un ex miembro del poder judicial que ya no se encontrara en el cargo o un profesional jurídico sénior con al menos diez años de experiencia que no fuera juez a tiempo completo. Los miembros judiciales fueron seleccionados de entre los miembros del poder judicial de Inglaterra y Gales, y la Oficina Judicial, en nombre del Presidente del Tribunal Supremo, gestionó el proceso de selección. La Oficina Judicial invitó a manifestar su interés de participar a los jueces del Tribunal Superior de Inglaterra y Gales y los participantes fueron entrevistados por un grupo de expertos, que estuvo integrado por el Presidente del IPT, un miembro no judicial del IPT y un Comisionado lego de la Comisión de Nombramientos del Poder Judicial. El grupo de expertos luego informó al Presidente del Tribunal Supremo que lo comunicó al Secretario de Estado del Interior realizando recomendaciones formales para los nombramientos. El Secretario de Estado del Interior escribió al Primer Ministro pidiéndole que solicitara permiso para emitir las Cartas Reales de Su Majestad la Reina para proceder a los nombramientos recomendados. El Primer Ministro recomendó los candidatos elegidos a Su Majestad la Reina, quien formalizó los nombramientos a través de las Cartas Reales. Los miembros no judiciales fueron seleccionados mediante concurso abierto. El IPT colocó anuncios para miembros no judiciales en una selección de periódicos nacionales y empresas de contratación para que manifestaran su interés personas debidamente cualificadas. El proceso se diferenciaba del de los miembros judiciales en que no involucraba al Presidente del Tribunal Supremo, pero era idéntico en todos los demás aspectos. Actualmente existen cinco miembros judiciales (dos miembros del Tribunal de Apelación Inglés (uno de los cuales es el Presidente), un miembro de Tribunal Superior y dos miembros de la Cámara Exterior del Tribunal Supremo de Escocia (uno de los cuales es el Vicepresidente) y cinco miembros no judiciales (de los cuales uno es un juez jubilado del Tribunal Superior Irlanda del Norte).

124. De acuerdo con las secciones 67 (2) y 67 (3) (c), el IPT debía aplicar los mismos principios aplicables por un tribunal a una solicitud de revisión judicial. Sin embargo, no tenía poder para hacer una declaración de incompatibilidad si consideraba que la legislación primaria era incompatible con el Convenio Europeo de Derechos Humanos,

ya que no era un "tribunal" a los efectos del artículo 4 de la Ley de Derechos Humanos de 1998.

125. La sección 68 (6) y (7) exigía a quienes participasen en la autorización y ejecución de una orden de interceptación revelar o proporcionar al IPT todos los documentos e información requeridos por éste.

126. La sección 68 (4) disponía que cuando el IPT admitiera una reclamación tenía el poder de otorgar una indemnización y de realizar cualquier otra consideración que estimara oportuna, incluida la declaración de anular o cancelar cualquier orden y requerir la destrucción de cualquier registro obtenido en virtud de la misma (sección 67 (7)). En el caso de que una reclamación planteada ante el IPT prosperara, por lo general, se requería que el IPT presentara un informe al Primer Ministro (sección 68 (5)).

127. La sección 68 (1) facultaba al IPT a establecer su propio procedimiento, sin perjuicio de que la sección 69 (1) disponía que el Secretario de Estado también podía establecer reglas de procedimiento.

2. El Reglamento del Tribunal de Poderes de Investigación de 2000 ("el Reglamento").

128. El Secretario de Estado aprobó el Reglamento en el que se regulaban varios aspectos relativos al procedimiento ante el IPT.

129. La Regla 9 permitía al IPT celebrar, en cualquier momento, vistas en las que el denunciante pudiera hacer declaraciones, presentar pruebas y citar a testigos. Aunque la Regla 9 disponía que los procedimientos del IPT, incluidas las vistas orales, se llevarían a cabo en privado, en los casos IPT / 01/62 e IPT / 01/77, el propio IPT decidió que, con sujeción al deber general impuesto por la Regla 6 (1) de prevenir la divulgación de información sensible, podría decidir discrecionalmente la celebración de una vista pública. Siguiendo este compromiso de celebrar vistas públicas cuando fuera posible, el IPT también ha publicado sus sentencias más significativas en su página web, siempre que no ha existido riesgo de divulgación de información perjudicial.

130. La Regla 11 permitía al IPT admitir pruebas en cualquier forma, incluso en supuestos en los que no serían admisibles ante un tribunal de justicia.

131. La Regla 6 exigía que el IPT desempeñara sus funciones de manera que se asegurara que no se divulgara información contraria al interés público o perjudicial para la seguridad nacional, la prevención o detección de delitos graves, el bienestar económico del Reino Unido o el desempeño de las funciones de cualquiera de los servicios de inteligencia.

3. Abogado del Tribunal

132. El IPT podía nombrar un abogado del Tribunal para realizar alegaciones en nombre de los demandantes en las vistas en las que no pudieran estar representados. En el caso Liberty, el abogado del Tribunal describió su papel como sigue:

> "El abogado del Tribunal desempeña una función diferente [a la de los abogados especiales en un proceso cerrado ante determinados tribunales], similar al *amicus curiae*. Su función es ayudar al Tribunal en la forma que éste le indique. A veces (por ejemplo, en relación con cuestiones en las que están representadas todas las partes), el Tribunal no especificará desde qué perspectiva se realizarán las alegaciones. En estas circunstancias, el abogado hará alegaciones de acuerdo con

su propio análisis de las cuestiones jurídicas o fácticas pertinentes, procurando hacer especial hincapié en los puntos que no han sido plenamente desarrollados por las partes. En otras ocasiones (en particular cuando uno o más intereses no estén representados), el Tribunal puede invitar a sus abogados a presentar alegaciones desde una perspectiva particular (normalmente la perspectiva de la parte o partes cuyos intereses no están representados de otra manera)".

133. Esta descripción fue aceptada y respaldada por el IPT.

4. R (sobre la demanda de Privacidad International) c. Tribunal de Poderes de Investigación y otros [2019] UKSC 22

134. En esta Sentencia, que fue dictada el 15 de mayo de 2019, el Tribunal Supremo sostuvo que la sección 67 (8) de la RIPA no impedía revisión judicial de una decisión del IPT.

E. Supervisión

135. En la Parte IV de la RIPA se preveía el nombramiento por el Primer Ministro de un Comisionado de Interceptación de Comunicaciones ("el Comisionado IC") y un Comisionado de los Servicios de Inteligencia encargado de la supervisión de las actividades de los servicios de inteligencia.

136. El Comisionado IC era el responsable de mantener bajo examen la interceptación de comunicaciones y la adquisición y divulgación de datos de comunicaciones por los servicios de inteligencia, fuerzas policiales y otras autoridades. Al llevar a cabo la revisión de las prácticas de vigilancia, el Comisionado de IC y sus inspectores tuvieron acceso a todos los documentos relevantes, incluidos los materiales cerrados, y todos los participantes en las actividades de interceptación tenían el deber de facilitarles cualquier material que requirieran. Las agencias interceptoras tenían la obligación de mantener registros que aseguraran que el Comisionado IC tuviera acceso efectivo a los detalles de las actividades de vigilancia realizadas. Después de cada inspección se enviaba un informe al responsable de la autoridad pública que contenía recomendaciones formales y que requería a la autoridad pública para que informara en un plazo de dos meses si las recomendaciones se habían aplicado o qué progresos se habían realizado. El Comisionado informa al Primer Ministro semestralmente respecto al desempeño de sus funciones y elaboraba un informe anual. Este informe era un documento público (sujeto a la no divulgación de los anexos confidenciales) que era presentado ante el Parlamento.

137. El Comisionado de los Servicios de Inteligencia llevó a cabo una vigilancia más independiente del uso de los poderes intrusivos de los servicios de inteligencia y dependencias del Ministerio de Defensa. Él también presentó informes anuales al Primer Ministro, que se presentaron ante el Parlamento.

138. La Ley de Poderes de Investigación de 2016 (véanse los párrafos 183 a 190 siguientes) derogó estas disposiciones, en la medida en que se referían a Inglaterra, Escocia y Gales, y en septiembre de 2017 la Oficina del Comisionado de poderes de investigación ("IPCO"- siglas en inglés-) asumió la responsabilidad de la supervisión de los poderes de investigación. La IPCO está formada por alrededor de quince Comisionados Judiciales, pertenecientes al Tribunal Superior actual y al recientemente suprimido, al Tribunal de apelación y al Tribunal Supremo; un grupo de Asesoramiento Técnico formado por expertos científicos; y casi cincuenta empleados, incluidos inspectores, abogados y expertos en comunicación.

F. Revisión de las operaciones de interceptación por parte del servicio de inteligencia.

1. Comité de Inteligencia y Seguridad del Parlamento ("ISC"- siglas en inglés-): Declaración de julio de 2013 sobre la presunta interceptación por la GCHQ de comunicaciones en el marco del programa PRISM de EEUU.

139. El ISC fue creado originariamente por la ISA para examinar la política, administración y gastos del MI5, el MI6 y la GCHQ. Desde la entrada en vigor de la Ley de Justicia y Seguridad de 2013, sin embargo, al ISC le fue expresamente concedida la condición de Comisión del Parlamento; le fueron proporcionadas mayores facultades; y su mandato se incrementó para incluir la supervisión de la actividad operativa y actividades más amplias de inteligencia y seguridad del Gobierno. De conformidad con las secciones 1 a 4 de la Ley de justicia y seguridad de 2013, estaba formado por nueve miembros procedentes de ambas Cámaras del Parlamento y, en el ejercicio de sus funciones, esos miembros tenían acceso rutinariamente a material altamente clasificado.

140. Tras las revelaciones de Edward Snowden, el ISC llevó a cabo una investigación sobre el acceso de la GCHQ al contenido de las comunicaciones interceptadas bajo el programa PRISM de los Estados Unidos, el marco legal que regía el acceso, y los acuerdos que la GCHQ tenía con sus contrapartes en el extranjero para compartir información. En el transcurso de la investigación, el ISC recibió evidencias detalladas de la GCHQ y discutió el programa con la NSA.

141. El ISC concluyó que las acusaciones de que la GCHQ había eludido la ley del Reino Unido mediante el uso del programa PRISM para acceder al contenido de las comunicaciones privadas eran infundadas ya que la GCHQ había cumplido con los deberes legales contenidos en la ISA. Además, concluyó que en cada caso en el que la GCHQ había solicitado información a los Estados Unidos, se había concedido una orden de interceptación, firmada por un Ministro del Gobierno.

2. Privacidad y seguridad: un marco legal moderno y transparente.

142. Tras su declaración de julio de 2013, el ISC llevó a cabo una investigación más profunda sobre el catálogo completo de facultades de los servicios de inteligencia. Su informe, que contenía una cantidad sin precedentes de información sobre las facultades intrusivas de los servicios de inteligencia, se publicó el 12 de marzo 2015.

143. El ISC consideró que los servicios de inteligencia y los servicios de seguridad no intentaron eludir la ley, incluidos los requisitos de la Ley de Derechos Humanos de 1998, que regían todas sus actuaciones. Sin embargo, consideró que, dado que el marco legal había desarrollado poco a poco, era innecesariamente complicado. Por tanto, el ISC tenía serias preocupaciones acerca de la falta de transparencia resultante, lo que no favorecía el interés público. En consecuencia, su recomendación clave fue que el marco legal existente fuera reemplazado por una nueva ley del Parlamento que estableciera claramente los poderes intrusivos de que disponen los servicios de inteligencia, los fines para los que podían utilizarlos, y la autorización requerida antes de que pudieran hacerlo.

144. Con respecto a la capacidad de interceptación masiva de la GCHQ, la investigación demostró que los servicios de inteligencia no tenían el poder legal, los recursos, la

capacidad técnica, o el deseo de interceptar cada comunicación de los ciudadanos británicos, o de Internet en su conjunto. La GCHQ, por lo tanto, no estaban leyendo los correos electrónicos de todo el Reino Unido. Por el contrario, los sistemas de interceptación masiva de la GCHQ operaban en un pequeño porcentaje de los portadores que componían Internet y el ISC consideró que la GCHQ aplicó niveles de filtrado y selección tales que sólo se acopió de cierta cantidad del material de esos portadores. Las búsquedas dirigidas aseguraron que solo aquellos elementos que se consideraban de más alto valor de inteligencia se exponían a los analistas para que los examinaran, con la consecuencia de que sólo una pequeña fracción de los mismos fueron vistos por ojos humanos.

145. Con respecto a las comunicaciones por Internet, el ISC consideró que la distinción entre comunicaciones "internas" y "externas" era confusa y carente de transparencia. Por tanto, sugirió que el Gobierno publicara una explicación de qué comunicaciones de Internet entraban dentro de cada categoría. No obstante, la investigación había desvelado que la interceptación masiva no podía utilizarse para interceptar las comunicaciones de un individuo en el Reino Unido sin una autorización específica, firmada por un Secretario de Estado, nombrando a ese individuo.

146. El ISC observó que la orden de la sección 8 (4) era muy breve. Aunque el certificado que la acompañaba establecía las categorías de comunicaciones que podían examinarse, esas categorías se expresaban en términos muy genéricos (por ejemplo, "material que proporciona inteligencia sobre terrorismo (como es definido por la Ley de Terrorismo de 2000 (conforme fue modificada)), incluyendo, entre otros, a organizaciones terroristas, terroristas, simpatizantes activos, planificación de ataques, recaudación de fondos"). Dado que el certificado era tan genérico, el ISC cuestionó si necesitaba ser secreto o si, en aras de la transparencia, podía ser publicado.

147. Aunque el certificado de la sección 8 (4) establecía las categorías generales de información que podían ser examinadas, el ISC constató que, en la práctica, era la selección de los portadores y la aplicación de selectores simples y criterios de búsqueda los que determinaban qué comunicaciones se examinaban. Por lo tanto, el ISC solicitó garantías de que estaban sujetos al escrutinio y revisión de los Ministros y / o los Comisionados. Sin embargo, las pruebas presentadas ante el ISC evidenciaron que ni los Ministros ni los Comisionados habían dado una importancia significativa a estos problemas. Por ende, el ISC recomendó que el Comisionado IC debería tener la responsabilidad legal de revisar los diversos criterios de selección utilizados en la interceptación masiva para garantizar que seguían lo previsto en el certificado y los requisitos válidos de seguridad nacional.

148. El ISC señaló que los datos de comunicaciones eran fundamentales para la mayoría de las investigaciones de los servicios de inteligencia: podían analizarse para encontrar patrones que reflejaban comportamientos particulares en línea asociados con actividades como planificación de ataques, para establecer vínculos, ayudaban a poner el foco en las personas que podrían plantear una amenaza, para asegurar que la interceptación se dirigía correctamente, y para detectar redes y asociaciones con relativa rapidez. Eran particularmente útiles en las primeras etapas de una investigación, cuando los servicios de inteligencia tenían que poder determinar si aquellas personas a las que se asociaba con un objetivo estaban conectadas con la trama (y por lo tanto requerían de una mayor investigación) o eran meros espectadores inocentes. Según el Secretario de Estado del

Departamento del Interior, habían "jugado un papel importante en todas las operaciones antiterroristas del Servicio de Seguridad durante la última década". Sin embargo, el ISC expresó su preocupación por la definición de "Datos de comunicaciones". Si bien aceptó que existía una categoría de datos de comunicaciones que era menos intrusiva y, por lo tanto, no requería el mismo grado de protección, consideró que existían ciertas categorías de datos de comunicaciones que tenían el potencial de revelar detalles más intrusivos sobre la vida privada de una persona y, por lo tanto, requerían de mayores salvaguardas.

149. Finalmente, en lo que respecta al IPT, el ISC reconoció expresamente la importancia de un derecho interno de apelación.

3. "Una cuestión de confianza": Informe de la revisión de las facultades de investigación por el Revisor Independiente de la Legislación de Terrorismo ("el Informe Anderson").

150. El Revisor Independiente de la Legislación de Terrorismo es una persona totalmente independiente del Gobierno, designada por el Secretario de Estado del Interior y Hacienda por un período renovable de tres años. Tiene encomendada la tarea de informar al Secretario de Estado del Interior y al Parlamento sobre el funcionamiento de la legislación antiterrorista en el Reino Unido. Estos informes se presentan ante el Parlamento para informar al público y para el debate político.

151. La finalidad del Informe Anderson, que se presentó ante el Parlamento y fue publicado el 11 de junio de 2015, y que lleva el nombre de David Anderson Q.C., el entonces Revisor Independiente de la Legislación de Terrorismo, era informar al público y el debate político sobre las amenazas a Reino Unido, las facultades necesarias para combatir esas amenazas, las salvaguardas para proteger la privacidad, los desafíos de la tecnología cambiante, cuestiones relacionadas con la transparencia y la supervisión, y la legislación nueva o modificada. Al realizar la revisión, el Revisor Independiente tenía acceso sin restricciones, al más alto nivel de autorización de seguridad, a los departamentos gubernamentales responsables y a las autoridades públicas. También a los proveedores de servicios, expertos técnicos independientes, organizaciones no gubernamentales, académicos, abogados, jueces y reguladores.

152. El Revisor Independiente señaló que el marco legal que regía los poderes de investigación se había "desarrollado de manera gradual", con la consecuencia de que había "pocas [leyes] más impenetrables que la RIPA y sus satélites".

153. Con respecto a la importancia de los datos relacionados con las comunicaciones, observó que permitieron a los servicios de inteligencia construir una imagen de las actividades de interés de un sujeto y fueron extremadamente importantes para proporcionar información sobre la actividad criminal y terrorista. Identificaron objetivos sobre los que trabajar y también ayudaron a determinar si alguien era completamente inocente. Era de especial importancia la posibilidad de utilizar datos de comunicaciones (sujetos a los requisitos de necesidad y proporcionalidad) para:

(a) vincular a un individuo a una cuenta o acción (por ejemplo, visitar un sitio web o enviar un correo electrónico) a través de su dirección IP;

(b) establecer el paradero de una persona, tradicionalmente a través de conexiones móviles o datos GPRS;

(c) establecer cómo se comunicaban los sospechosos o las víctimas (a través de qué aplicaciones o servicios);

(d) observar la delincuencia en línea (por ejemplo, qué sitios web fueron visitados con fines de terrorismo, la explotación sexual de niños o compra de armas de fuego o drogas ilegales); y

(e) utilizar los datos (por ejemplo, para identificar dónde, cuándo y con a quién o qué se estaba comunicando alguien, cómo un programa malicioso o un ataque de denegación de servicio se ha llevado a cabo, y para corroborar otras evidencias).

154. Además, se podía realizar el análisis de datos de comunicaciones rápidamente, haciéndolos extremadamente útiles en operaciones de movimiento rápido, y el uso de los datos de las comunicaciones podía evitar el uso de un sistema más intrusivo, o proporcionar la información que haría que otras medidas fueran innecesarias.

155. Las propuestas de reforma del Revisor Independiente pueden resumirse en las siguientes:

(a) la redacción de una nueva ley completa y comprensible, reemplazando "la multitud de poderes actuales" y proporcionando unos límites y salvaguardas claros sobre cualquier poder intrusivo cuyo uso pueda ser necesario por las autoridades públicas;

(b) la revisión y aclaración de las definiciones de "contenido" y "datos de comunicaciones";

(c) el mantenimiento de la facultad de los servicios de seguridad e inteligencia de practicar la recolección masiva de material interceptado y datos asociados a las comunicaciones, pero sujeta a estrictas salvaguardas adicionales, incluyendo la autorización de todas las órdenes por un Comisionado Judicial en una nueva Comisión de Vigilancia Independiente e Inteligencia ("ISIC" – siglas en inglés-);

(d) la concreción en el certificado adjunto de los fines para los cuales el material o los datos se buscaron por referencia a operaciones específicas o fines de la misión (por ejemplo, "planificación de ataques por ISIL en Irak / Siria contra el Reino Unido");

(e) la creación de un nuevo tipo de orden de interceptación masiva limitada a la adquisición de datos de comunicaciones que en determinados casos puedan ser una opción proporcionada;

(f) la ISIC debería asumir las funciones de supervisión de inteligencia y debería ser pública, transparente y accesible a los medios de comunicación;

y

(g) el IPT debería tener competencia para hacer declaraciones de incompatibilidad y sus fallos deberían poder ser objeto de recurso de conformidad con la ley.

4. Una licencia democrática para operar: Informe de Revisión Independiente de la Vigilancia ("ISR"-siglas en inglés-).

156. El ISR fue realizado por el Instituto Real de Servicios Unidos, un grupo de reflexión independiente, a petición del entonces Viceprimer Ministro, en parte en respuesta a las revelaciones de Edward Snowden. Sus atribuciones eran las de examinar la legalidad de los programas de vigilancia del Reino Unido y la efectividad de los regímenes que los regían, y sugerir las reformas que pudieran ser necesarias para proteger tanto la privacidad individual como las facultades necesarias de la policía y los servicios de seguridad e inteligencia.

157. Habiendo completado su revisión, el ISR no encontró evidencia alguna de que el Gobierno Británico estuviera actuando a sabiendas de manera ilegal al interceptar comunicaciones, o de que la facultad de recopilar datos en masa que estaba siendo utilizada por el Gobierno le proporcionara una ventana perpetua a la vida privada de ciudadanos británicos. En cambio, si consideró que el marco legal existente que autorizaba a la interceptación de comunicaciones era confuso, no había seguido el ritmo de los avances en la tecnología de las comunicaciones, y no servía ni al Gobierno ni a los ciudadanos satisfactoriamente. Por lo tanto, concluyó que era necesario un marco legal nuevo, completo y más claro.

158. En particular, apoyó la opinión expuesta tanto en el ISC como en el Informe Anderson de que, si bien se precisaba de los poderes de vigilancia actuales, se necesitaban tanto un nuevo marco legislativo como un nuevo régimen de supervisión. Consideró además que las definiciones de “contenido” y “datos de comunicaciones” debían revisarse en el borrador de la nueva legislación para que pudieran delimitarse claramente en la ley.

159. Con respecto a los datos de comunicaciones, el informe señaló que ponían a disposición un mayor volumen de información del individuo que el contenido, porque cada parte del contenido estaba rodeada de múltiples piezas de datos de comunicaciones. Además, poniendo en relación los conjuntos de datos se podía crear una imagen extremadamente precisa de la vida de un individuo, si se contaba con los suficientes datos sin procesar, algoritmos y ordenadores potentes podían generar una imagen sustancial del individuo y sus patrones de comportamiento sin ni siquiera acceder al contenido. Además, el uso de métodos de cifrado cada vez más sofisticados había hecho que cada vez fuera más difícil acceder al contenido.

160. Consideró además que la facultad de los servicios de seguridad y de inteligencia de recopilar y analizar material interceptado de forma masiva debía mantenerse, pero con salvaguardas más estrictas conforme a lo recomendado en el Informe Anderson. En particular, consideró que las órdenes de interceptación masiva debían ser mucho más detalladas y ser objeto de un proceso judicial de autorización, salvo cuando el requerimiento fuera urgente.

161. Además, estuvo de acuerdo tanto con el ISC como con el Informe Anderson en que debería haber diferentes tipos de órdenes de interceptación y adquisición de comunicaciones y datos relacionados. Propuso que las órdenes para un fin relacionado con la detección o prevención de delitos graves y el crimen organizado siempre debían estar autorizadas por un Comisionado Judicial, mientras que las órdenes para fines relacionados con la seguridad nacional debían ser autorizadas por el Secretario de Estado y estar sujetas a revisión judicial por un Comisionado Judicial.

162. Con respecto al IPT, el ISR recomendó que las vistas fueran públicas, excepto cuando las vistas a puerta cerrada fueran necesarias en interés de la justicia o por otro motivo de interés público identificable. Además, el IPT debería tener la capacidad de testar las evidencias secretas presentadas ante él, posiblemente mediante el nombramiento de un Asesor Especial. Finalmente, coincidió con el ISC y el Informe Anderson sobre que un derecho de apelación nacional era importante y debería tenerse en cuenta en la legislación futura.

5. Informe de Revisión de los poderes masivos.

163. La revisión de los poderes masivos se estableció en mayo de 2016 para evaluar la forma de ejecutar los cuatro poderes masivos contenidos en lo que entonces era el Proyecto de Ley de Poderes de Investigación (ahora Ley de Poderes de Investigación de 2016: ver párrafos 183-190 siguientes). Esos poderes estaban relacionados con la interceptación masiva y la adquisición masiva de datos de comunicaciones, la interferencia masiva de equipos y la adquisición masiva de conjuntos de datos personales.

164. El examen fue realizado nuevamente por el Revisor Independiente de la Legislación sobre Terrorismo. Para realizar la revisión reclutó a tres miembros para su equipo, todos los cuales tenían la autorización de seguridad necesaria para acceder a material altamente clasificado, incluyendo a una persona con los conocimientos técnicos necesarios para comprender los sistemas y técnicas utilizados por la GCHQ, y los usos que se les podían dar; un investigador con experiencia como usuario de inteligencia secreta, incluyendo la inteligencia generada por la GCHQ; y un abogado sénior independiente con las habilidades y la experiencia para valorar las evidencias forenses y los estudios presentados por los servicios de seguridad y de inteligencia.

165. Al realizar su examen, el equipo mantuvo un importante y detallado contacto con los servicios de inteligencia en todos los niveles de antigüedad, así como órganos de supervisión pertinentes (incluido el IPT y los abogados del Tribunal), ONGs y expertos técnicos independientes.

166. Aunque la revisión la realizó sobre el Proyecto de Ley de Poderes de Investigación, varios de sus hallazgos con respecto a la interceptación masiva fueron relevantes para el caso en cuestión. En particular, tras haber examinado una gran cantidad de material cerrado, la revisión concluyó que la interceptación masiva era una facultad esencial: primero, porque los terroristas, criminales y los servicios de inteligencia extranjeros hostiles se habían vuelto cada vez más sofisticados para evadir la detección por medio de los métodos tradicionales; y en segundo lugar, porque la propia naturaleza de Internet implicaba que la ruta por la que viajaría una comunicación en particular se había vuelto enormemente impredecible. El equipo de revisión analizó alternativas a la interceptación masiva (incluida la interceptación dirigida, el uso de fuentes humanas y productos comerciales de ciber-defensa), pero concluyó que ninguna alternativa o combinación de alternativas eran suficientes para sustituir el poder de la interceptación masiva como método para obtener la inteligencia necesaria.

6. Ataques en Londres y Manchester marzo-junio de 2017: Evaluación independiente del MI5 y revisiones internas de la policía.

167. Tras una serie de cuatro ataques terroristas en el breve período comprendido entre marzo y junio de 2017, en el curso de los cuales unas treinta y seis personas inocentes fallecieron y casi 200 más resultaron heridas, el Secretario de Estado de Interior pidió al Revisor Independiente sobre la Legislación de Terrorismo recientemente retirado, David Anderson Q.C., que evaluara las revisiones internas clasificadas de la policía y los servicios de inteligencia implicados. Al contextualizar los ataques, el Informe contenía las siguientes observaciones:

> ‘‘1.4 Primero, el ***nivel de amenaza*** en el Reino Unido por el llamado 'terrorismo internacional' (en la práctica, terrorismo islamista, ya sea generado en el país o en el extranjero) ha sido evaluado por el Centro Conjunto de Análisis del Terrorismo (JTAC) como SEVERO desde agosto de 2014, lo que indica que los ataques terroristas islamistas en el Reino Unido son “muy probables”. Los analistas con acceso a la inteligencia relevante siempre han tenido claro que dicha evaluación es realista. También han señalado la amenaza más pequeña pero aún mortal del terrorismo de extrema derecha (XRW), ejemplificada por el asesinato del diputado Jo Cox en junio de 2016 y por la proscripción del grupo neonazi Acción Nacional en diciembre de 2016.
>
> 1.5 En segundo lugar, el ***creciente aumento*** de la amenaza de terrorismo islamista es sorprendente. El director general del MI5, Andrew Parker, habló en octubre de 2017 de “un dramático cambio al alza en la amenaza de este año al ritmo más alto que he visto en mis 34 años de carrera”. Aunque las muertes por terrorismo islamista ocurren de manera abrumadora en África, el Medio Oriente y Asia meridional, la amenaza ha aumentado recientemente en todo el mundo occidental y ha sido descrita como “especialmente difusa y diversa en el Reino Unido”. Queda por ver cómo esta tendencia se verá afectada, para bien o para mal, por el colapso físico del llamado Estado Islámico en Siria e Irak.
>
> 1.6 En tercer lugar, los ***perfiles de los atacantes*** ... muestran muchas características similares ...
>
> 1.7 En cuarto lugar, aunque los ***objetivos*** de los tres primeros ataques no se extendieron a todo el rango actual, tenían fuertes similitudes con los objetivos de otros ataques occidentales recientes: centros políticos (por ejemplo, Oslo 2011, Ottawa 2014, Bruselas 2016); asistentes a conciertos, juerguistas y multitudes (por ejemplo, Orlando 2016, París 2016, Barcelona 2017); y policías oficiales (por ejemplo, Melbourne 2014, Berlín 2015, Charleroi 2016). Hay precedentes también de ataques a musulmanes practicantes que han cruzado la frontera del delito de odio al terrorismo, incluyendo el asesinato de Mohammed Saleem en West Midlands en 2013.
>
> 1.8 En quinto lugar, el ***modus operandi*** (MO) de los ataques terroristas se ha diversificado y simplificado a lo largo de los años, ya que el Daesh ha empleado su gran esfuerzo de propaganda para inspirar más que dirigir actos de terrorismo en Occidente. Los ataques bajo revisión cuentan con similitudes en relación con el tiempo y lugar:
>
> (a) A diferencia de los grandes complots islamistas dirigidos característicos de la última década, los cuatro ataques fueron cometidos por ***actores solitarios*** o ***pequeños grupos***, con poca evidencia de planificación detallada o con de un objetivo preciso.
>
> (b) Los fuertes controles de armas en el Reino Unido implican que las ***armas blancas*** sean más comúnmente utilizadas que las armas de fuego en delitos terroristas y relacionados con pandillas.
>
> c) Desde que un camión mató a 86 personas inocentes en Niza (julio de 2016), los ***vehículos***, que aparecen en tres de los cuatro ataques bajo revisión, se han utilizado cada vez más como armas.
>
> (d) La ***combinación*** de un vehículo y armas blancas, vista en Westminster y London Bridge, se había utilizado previamente para matar al soldado Lee Rigby (Woolwich, 2013).
>
> (e) Los ***explosivos***, utilizados en Manchester, eran el arma más popular para los terroristas islamistas contra Europa entre 2014 y 2017. Se ha demostrado que el explosivo TATP puede ser fabricado (con la ayuda de compras en línea e instrucciones de montaje) más fácilmente de lo que se suponía”.

7. Informe anual del Comisionado de Interceptación de Comunicaciones de 2016.

168. El Comisionado IC observó que al realizarse la interceptación bajo una orden de la sección 8 (4), una agencia de interceptación tenía que usar sus conocimientos sobre la forma en que se llevaban a cabo las comunicaciones internacionales, combinados con encuestas periódicas de enlaces de comunicaciones relevantes, para identificar aquellos portadores de comunicaciones individuales que tenían más probabilidades de contener comunicaciones externas que cumplieran con las descripciones del material certificado por el Secretario de Estado bajo la sección 8 (4). También tenía que realizar la interceptación de forma que se limitara la recopilación de comunicaciones al nivel mínimo compatible con el objetivo de interceptar las comunicaciones externas deseadas.

169. Observó además que antes de que los analistas puedan leer, visualizar o escuchar el material, tenían que proporcionar una justificación, que incluía el por qué se requería el acceso al material, que fuera conforme con la sección 16 y el certificado correspondiente, y de por qué dicho acceso era proporcionado. Las inspecciones y auditorías mostraron que, aunque el procedimiento de selección fue llevado a cabo cuidadosa y concienzudamente, se basó en el juicio profesional de los analistas, su formación y la supervisión de la gestión.

170. Según el informe, se emitieron 3007 órdenes de interceptación en 2016 y cinco solicitudes fueron rechazadas por el Secretario de Estado. En la opinión del Comisionado IC, estas cifras no capturaban la calidad crítica de la función de aseguramiento inicialmente llevada a cabo por el personal y los abogados de la agencia interceptora o el departamento de concesión de órdenes (los departamentos de concesión de órdenes eran una fuente de asesoramiento independiente para el Secretario Estado y realizaban un escrutinio previo a la autorización de las solicitudes y sus renovaciones para asegurar que fueran (y siguieran siendo) necesarias y proporcionadas). Basándose en sus inspecciones, estaba convencido de que el bajo número de rechazos reflejaba la cuidadosa consideración dada al uso de estos poderes.

171. Una inspección típica de una agencia de interceptación incluía lo siguiente:

- una revisión de los puntos de acción o recomendaciones de la inspección previa y su implementación;
- una evaluación de los sistemas existentes para la interceptación de comunicaciones para garantizar que fueran suficientes conforme a los fines del Capítulo 1, Parte 1 de la RIPA y de que todos los registros pertinentes se hubieran conservado;
- el examen de las solicitudes de interceptación seleccionadas para evaluar si eran necesarias en primera instancia y si las solicitudes cumplieron los requisitos de necesidad y proporcionalidad;
- entrevistas con los agentes encargados del caso, analistas y / o lingüistas de las investigaciones u operaciones seleccionadas para evaluar si la interceptación y las justificaciones para adquirir todo el material fueron proporcionadas;
- el examen de cualquier aprobación oral urgente para comprobar que el proceso se justificó y se utilizó de manera apropiada;

- una revisión de aquellos casos en los que las comunicaciones sujetas a privilegio legal o información confidencial había sido interceptada y retenida, y cualquier caso en el que un abogado fuera el sujeto de una investigación;
- una revisión de la idoneidad de las salvaguardas y las disposiciones adoptadas bajo las secciones 15 y 16 de la RIPA;
- una investigación de los procedimientos establecidos para la retención, almacenamiento y destrucción del material interceptado y de los datos relacionados con las comunicaciones; y
- una revisión de los errores notificados, incluida la verificación de que las medidas adoptadas para prevenir la recurrencia fueron suficientes.

172. Después de cada inspección, los inspectores elaboraban un informe que incluía:

- una evaluación de hasta qué punto las recomendaciones de la anterior inspección se habían implementado;
- un resumen del número y tipo de documentos de interceptación seleccionados para inspección, incluida una lista detallada de esas órdenes;
- comentarios detallados sobre todas las autorizaciones seleccionadas para su mayor examen y debate durante la inspección;
- una evaluación de los errores notificados a la oficina del Comisionado IC durante el período que era objeto de inspección;
- consideraciones sobre los procedimientos de retención, almacenamiento y destrucción;
- consideraciones sobre otras cuestiones de política u operativas de la agencia o departamentos que otorgan las órdenes planteadas durante la inspección;
- una evaluación de cómo cualquier material sujeto a privilegio legal profesional (o cualquier otro material confidencial) se había manejado; y
- una serie de recomendaciones destinadas a mejorar el cumplimiento y rendimiento.

173. Durante 2016, la oficina del Comisionado IC inspeccionó una vez a las nueve agencias de interceptación y a los cuatro departamentos principales que otorgan órdenes de interceptación dos veces. Esto, junto con visitas adicionales a la GCHQ, hicieron un total de veintidós visitas de inspección. Además, él y sus inspectores organizaron otras visitas *ad hoc* a las agencias.

174. La inspección de los sistemas establecidos para solicitar y autorizar las órdenes de interceptación generalmente comprendían un proceso de tres etapas. Primero, para lograr una muestra representativa de órdenes, los inspectores seleccionaron diferentes tipos de delitos y amenazas a la seguridad nacional. Además, los inspectores se centraron en aquéllas de especial interés o sensibilidad (como las que dieron lugar a un grado inusual de intrusión colateral, las que se habían mantenido durante un período considerable, las que fueron aprobadas oralmente, las que tuvieron como resultado la interceptación de comunicaciones legamente protegidas o confidenciales, y las llamadas órdenes "temáticas"). En segundo lugar, los inspectores examinaban en detalle las órdenes seleccionadas y la documentación asociada durante los días de lectura que precedían a las inspecciones. En este punto, los inspectores pudieron examinar las declaraciones de necesidad y proporcionalidad realizadas por los analistas al agregar un selector al sistema de recolección para examen. Cada declaración tenía que sostenerse

por sí misma y tenía que estar referida al requisito general de prioridades para la recopilación de inteligencia. En tercer lugar, identificaron aquellas órdenes, operaciones o áreas del proceso de las que requerían mayor información o aclaraciones y concertaron citas para entrevistar al personal operativo, legal o técnico pertinente. Cuando era necesario, examinaban más a fondo la documentación o sistemas relacionados con esas órdenes.

175. Se examinaron novecientas setenta órdenes durante las veintidós inspecciones de interceptación (el 61% del número de órdenes vigentes al final del año y el 32% del total de nuevas órdenes emitidas en 2016).

176. Los períodos de retención no estaban prescritos en la legislación, pero las agencias tenían que tomar en consideración lo previsto en la sección 15 (3) de la RIPA, que disponía que el material o los datos tenían que ser destruidos tan pronto como ya no fuera necesario retenerlos para cualquiera de los fines autorizados en la sección 15 (4). De acuerdo con el informe, cada agencia de interceptación tenía una opinión diferente sobre lo que se consideraba un período de retención apropiado para el material interceptado y datos de las comunicaciones. Por lo tanto, los períodos de retención diferían dentro de las agencias de interceptación; respecto al contenido, oscilaron entre treinta días y un año, y respecto a los datos de comunicaciones, oscilaron entre seis meses y un año. En la práctica, sin embargo, la mayor parte del contenido fue revisado y eliminado automáticamente después de un período de tiempo muy corto a menos que se llevara a cabo alguna acción específica para retenerlo durante más tiempo porque fuera necesario.

177. El Comisionado IC señaló expresamente que "quedó impresionado por la calidad" de las declaraciones de necesidad y proporcionalidad realizadas por los analistas al agregar un selector al sistema de recolección para su examen.

178. Los inspectores formularon un total de veintiocho recomendaciones en sus informes de inspección, dieciocho de las cuales se realizaron en relación con el proceso de solicitud. La mayoría de las recomendaciones en esta categoría estaban relacionadas con la necesidad, la proporcionalidad y / o las justificaciones de intrusión colateral en las solicitudes, o el manejo de material legalmente privilegiado u otro tipo de material confidencial relacionado con profesiones sensibles.

179. El número total de errores de interceptación notificados al Comisionado IC durante 2016 fue de 108. La causa principal de los errores de interceptación fueron las recopilaciones excesivas (generalmente errores técnicos de software o hardware que provocaron una recopilación excesiva de material interceptado y datos de comunicaciones), selección / examen no autorizado, difusión incorrecta, no cancelar la interceptación, y la interceptación de las comunicaciones de una dirección o de una persona incorrecta.

180. Finalmente, con respecto al intercambio de inteligencia, el Comisionado IC observó que:

> "La GCHQ proporcionó detalles completos de los acuerdos de intercambio mediante los cuales los socios de los Cinco Ojos pueden acceder a elementos resultantes de las órdenes de interceptación ejecutadas por la GCHQ mediante sus propios sistemas. Mis inspectores también se reunieron con representantes de los Cinco Ojos y recibieron una demostración de cómo otros miembros de los Cinco Ojos podían solicitar acceso a los datos de la GCHQ. El acceso a los

sistemas de la GCHQ está estrictamente controlado y tiene que estar justificado de acuerdo con las leyes del país anfitrión y las instrucciones de uso de las salvaguardas de las secciones 15/16. Antes de tener acceso a los datos de la GCHQ, los analistas de los Cinco Ojos deben completar el mismo proceso de capacitación legal que el personal de la GCHQ ".

8. Informe anual del Comisionado de Servicios de Inteligencia para 2016

181. El Comisionado de Servicios de Inteligencia, en su informe sobre el cumplimiento de la "Guía consolidada para oficiales de inteligencia y personal al servicio para la detención y entrevistas de detenidos en el extranjero, y sobre la transmisión y recepción de información de inteligencia relacionada con los detenidos", observó que:

"En el curso de su trabajo, cada una de las agencias trabaja en estrecha colaboración con socios de cooperación extranjeros. Esto implica compartir inteligencia de forma rutinaria y, a veces, colaborar en operaciones. Considero que las agencias son sensibles a las implicaciones de trabajar con socios que actúan bajo diferentes sistemas legales y que [los servicios de inteligencia del Reino Unido] que trabajan en el extranjero son cuidadosos en cuanto a la aplicación de los principios legales del Reino Unido en la medida de lo posible.

...

La GCHQ trabaja en estrecha colaboración con socios de enlace y participa regularmente compartiendo inteligencia y en ocasiones con trabajos colaborativos. Esta es un área compleja tanto para la GCHQ como para el SIS, donde el personal de la agencia trabaja con socios que aplican diferentes marcos legales y, a veces, incompatibles. Me han impresionado los esfuerzos del personal de la GCHQ para obtener garantías de los socios, en particular con respecto a la Guía consolidada. He recomendado que la GCHQ debería considerar hacer referencia en cualquier presentación pertinente al hecho de que las leyes locales serán aplicables a la actividad de cualquier socio.

Estoy satisfecho de que la GCHQ esté aplicando los principios de la guía consolidada con sensibilidad, y me complace que los cambios realizados en la capacitación del personal las 24 horas del día, los 7 días de la semana estén aumentando el ya alto nivel del proceso de referencia. Aprecié que en ocasiones los funcionarios de la GCHQ actualizaron el registro con posterioridad para aclarar juicios o detalles. Si bien es importante representar los datos disponibles de forma más completa, recomendé que la GCHQ estableciera puntos de aclaración y no enmiendas a las entradas del registro original. La GCHQ confirmó posteriormente que esto se había implementado.

...

El Secretario de Estado de Relaciones Exteriores también es responsable de proporcionar supervisión ministerial sobre las ocasiones en las que se ha aplicado la guía consolidada y las agencias tienen la intención de continuar, ya sea con el intercambio de inteligencia o con una operación en vivo. He recomendado que el [Ministerio de Relaciones Exteriores y de la Mancomunidad de Naciones] debe obtener una copia de las garantías que el SIS haya obtenido de un socio de enlace. Aconsejaría que éstas fueran puestas a disposición del Secretario de Relaciones Exteriores para su escrutinio al considerar cualquier alegación relacionada con la guía consolidada".

182. La supervisión del cumplimiento de la Guía consolidada recae ahora bajo las funciones del nuevo Comisionado de Poderes de Investigación. Actualmente se está revisando la Guía desde que el Comisionado de los Servicios de Inteligencia, en su informe de 2015, indicó que, si bien "no pensaba que la Guía consolidada fuera fundamentalmente defectuosa o no cumpliera su fin", sin embargo, consideraba que había estado "en funcionamiento en su forma actual durante algunos años y que había espacio para la mejora".

G. La Ley de Poderes de Investigación de 2016.

183. La Ley de Poderes de Investigación de 2016 recibió la sanción real el 29 de noviembre de 2016. El nuevo régimen que introducido es ahora mucho más operativo, habiendo entrado en vigor durante el transcurso de 2018.

184. En virtud de la Ley de 2016, una orden de interceptación masiva -que podía cubrir tanto el "contenido" de las comunicaciones como los "datos secundarios" - tenía que ser necesaria al menos en interés de la seguridad nacional (pero también podía ser necesaria con el fin de prevenir o detectar delitos graves o en interés del bienestar económico del Reino Unido en la medida en que esos intereses sean también relevantes para los intereses de la seguridad nacional). La orden debe especificar los "fines operativos" conforme a los cuales cualquier material obtenido en virtud de esa orden pueden ser seleccionado para examen. Hay disposiciones detalladas sobre la elaboración de la lista de "fines operativos" por parte de los altos cargos de los servicios de inteligencia. Un fin operativo puede especificarse en esa lista solo con la aprobación del Secretario de Estado. La lista de fines operativos debe remitirse al ISC cada tres meses y debe ser revisada por el Primer Ministro al menos una vez al año.

185. La solicitud de una orden de interceptación masiva debe ser realizada por o en nombre de un alto cargo de un servicio de inteligencia. El poder de emitir una orden debe ser ejercido personalmente por el Secretario de Estado y para decidir si emitir una orden masiva, debe aplicar los principios de necesidad y proporcionalidad. La emisión de la orden está sujeta a la aprobación previa de un Comisionado Judicial, quien debe aplicar los principios de revisión judicial (el llamado "doble bloqueo"). Por tanto, el Comisionado Judicial debe valorar por sí mismo cuestiones tales como si la interceptación está justificada por ser proporcionada en virtud del artículo 8.2 del Convenio.

186. La orden tiene una duración de seis meses a menos que sea cancelada o renovada. La renovación está sujeta a la aprobación de un Comisionado Judicial.

187. El "fin principal" de la orden debe ser obtener "comunicaciones relacionadas con el extranjero", que son las comunicaciones enviadas o recibidas por personas fuera de las Islas Británicas. La selección para el examen del contenido interceptado o "material protegido" está sujeto a la "salvaguarda de las Islas Británicas", lo que significa que no se puede seleccionar en ningún momento para su examen si alguno de los criterios utilizados para la selección del contenido interceptado remite a un individuo que se conoce que se encuentra en ese momento en el Islas Británicas, y el fin de usar esos criterios es identificar el contenido de las comunicaciones enviadas por, o destinadas a, ese individuo.

188. La Ley de 2016 también creó un recurso de apelación ante el IPT y reemplazó al Comisionado de Interceptación de Comunicaciones por el nuevo Comisionado de Poderes de Investigación (véase el párrafo 138 anterior).

189. Una serie de nuevos códigos de prácticas, incluido un nuevo Código de prácticas para la interceptación de comunicaciones, entraron en vigor el 8 de marzo de 2018 (ver párrafo 102 anterior).

190. La Parte 4 de la Ley de 2016, que entró en vigor el 30 de diciembre 2016, incluyó la facultad de emitir "avisos de retención" a los operadores de telecomunicaciones

requiriéndoles la retención de datos. Después de la impugnación legal de Liberty, el Gobierno reconoció que la Parte 4 de la Ley de 2016 era, tal y como estaba redactada, incompatible con los requisitos de la legislación de la UE. La Parte 4 no fue enmendada y el 27 de abril de 2018, el Tribunal Superior determinó que la Parte 4 era incompatible con los derechos fundamentales previstos en la legislación de la UE ya que, en el ámbito de la justicia penal, el acceso a los datos retenidos no se limitó al fin de combatir los "delitos graves"; y el acceso a los datos retenidos no estaba sujeto a la revisión previa por un tribunal o un organismo administrativo independiente.

II. DERECHO INTERNACIONAL APLICABLE

A. Naciones Unidas.

191. La Resolución núm. 68/167, aprobada por la Asamblea General el 18 de diciembre de 2013, establece lo siguiente:

> "La Asamblea General,
>
> ...
>
> 4. Exhorta a todos los Estados a que:
>
> ...
>
> (c) Examinen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad, velando por que se dé cumplimiento pleno y efectivo de todas sus obligaciones en virtud del derecho internacional de los derechos humanos;
>
> (d) Establezcan o mantengan mecanismos nacionales de supervisión independientes y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado."

B. El Consejo de Europa

1. El Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.

192. El Convenio, que entró en vigor para Reino Unido el 1 de diciembre de 1987, configura los estándares de protección de datos en el ámbito del tratamiento automático de datos personales en el sector público y privado. Dispone, a los efectos que aquí nos conciernen que:

> "
>
> **Preámbulo**
>
> Los Estados miembros del Consejo de Europa, signatarios del presente Convenio;
>
> Considerando que el fin del Consejo de Europa es llevar a cabo una unión más íntima entre sus miembros, basada en el respeto particularmente de la preeminencia del derecho así como de los derechos humanos y de las libertades fundamentales;
>
> Considerando que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados;

Reafirmando al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras;

Reconociendo la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos,

Convienen en los siguiente:

Artículo 1 - Objeto y fin.

El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»)

....

Artículo 8. Garantías complementarías para la persona concernida.

Cualquier persona deberá poder:

a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;

b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;

c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio;

d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, que se refieren los párrafos b) y c) del presente artículo.

Artículo 9. Excepción y restricciones.

1. No se admitirá excepción alguna en las disposiciones de los artículos 5, 6 y 8 del presente Convenio, salvo que sea dentro de los límites que se definen en el presente artículo.

2. Será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente Convenio cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática:

a) Para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales;

b) para la protección de la persona concernida y de los derechos y libertades de otras personas.

... “

Artículo 10 - Sanciones y recursos.

Cada Parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de estas disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos enunciados en el presente capitulo.”.

193. El Informe explicativo del Convenio antes mencionado explica que:

Artículo 9 - Excepciones y restricciones

"55. Las excepciones a los principios básicos de protección de datos se limitan a aquéllas que son necesarias para la protección de los valores fundamentales en una sociedad democrática. El texto del segundo párrafo de este artículo se ha modelado a partir del segundo párrafo de los artículos 6, 8, 10 y 11 del Convenio Europeo de Derechos Humanos. Se desprende de las decisiones de la Comisión y el Tribunal de Derechos Humanos relativas al concepto de "medidas necesarias" que los criterios para este concepto no pueden establecerse para todos los países y todas las épocas, sino que deben considerarse a la luz de la situación de cada país.

56. En el párrafo 2 se enumeran los principales intereses del Estado que pueden requerir excepciones. Estas excepciones son muy específicas para evitar que, en lo que respecta a la aplicación general del Convenio, los Estados tengan un margen de maniobra indebidamente amplio.

Los Estados conservan, en virtud del artículo 16, la posibilidad de rechazar la aplicación del Convenio en casos individuales por razones importantes, que incluyen las enumeradas en Articulo 9.

La noción de "seguridad del Estado" debe entenderse en el sentido tradicional de proteger la soberanía nacional contra amenazas internas o externas, incluida la protección de las relaciones internacionales del Estado".

2. El Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos, hecho en Estrasburgo el 8 de noviembre de 2001 (CETS Núm. 181)

194. El Protocolo, que no ha sido ratificado por el Reino Unido, establece, a los efectos que aquí nos conciernen que:

Artículo 1. Autoridades de control.

1. Cada Parte dispondrá que una o más autoridades sean responsables de garantizar el cumplimiento de las medidas previstas por su derecho interno que hacen efectivos los principios enunciados en los Capítulos II y III del Convenio, así como en el presente Protocolo.

2. a A este efecto, las autoridades mencionadas dispondrán, en particular, de competencias para la investigación y la intervención, así como de la competencia para implicarse en las actuaciones judiciales o para llamar la atención de las autoridades judiciales competentes respecto de las violaciones de las disposiciones del derecho interno que dan efecto a los principios mencionados en el apartado 1 del artículo 1 del presente Protocolo.

b. Cada autoridad de control atenderá las reclamaciones formuladas por cualquier persona en relación con la protección de sus derechos y libertades fundamentales respecto de los tratamientos de datos de carácter personal dentro de su competencia.

3. Las autoridades de control ejercerán sus funciones con total independencia.

4. Las decisiones de las autoridades de control que den lugar a reclamaciones podrán ser objeto de recurso ante los tribunales.

... "

Artículo 2. Flujos transfronterizos de datos de carácter personal hacia un destinatario que no está sujeto a la jurisdicción de una Parte en el Convenio.

1. Cada Parte dispondrá que la transferencia de datos de carácter personal hacia un destinatario sometido a la jurisdicción de un Estado u organización que no sea Parte en el Convenio sólo podrá efectuarse si dicho Estado u organización garantiza un nivel de protección adecuado a la transferencia de datos prevista.

2. No obstante lo dispuesto en el apartado 1 del artículo 2 del presente Protocolo, cada Parte podrá permitir la transferencia de datos de carácter personal:

a. si está prevista en su legislación interna a causa de:

intereses específicos de la persona interesada, o de

intereses legítimos prevalecientes, en particular, intereses públicos importantes, o

b. si la persona responsable de la transferencia ofrece garantías, que, en particular, pueden resultar de cláusulas contractuales, y éstas son juzgadas suficientes por la autoridad competente de conformidad con el derecho interno.".

3. Recomendación del Comité de Ministros sobre la protección de datos personales en el ámbito de los servicios de telecomunicaciones.

195. La Recomendación (núm. R (95) 4 del Comité de Ministros), que fue adoptada el 7 de febrero de 1995, establece, a los efectos que aquí nos conciernen, lo siguiente:

"2.4. La interferencia de las autoridades públicas en el contenido de una comunicación, incluyendo el uso de dispositivos de escucha o intervención u otros medios de vigilancia o de interceptación de comunicaciones, debe realizarse sólo cuando así lo disponga ley y constituya una medida necesaria en una sociedad democrática en interés de:

a. proteger la seguridad del estado, la seguridad pública, los intereses monetarios del Estado o la represión de delitos penales;

b. proteger al interesado o los derechos y libertades de otros.

2.5. En el caso de injerencia de las autoridades públicas en el contenido de una comunicación, la legislación nacional debería regular:

a. el ejercicio de los derechos de acceso y rectificación del interesado;

b. en qué circunstancias las autoridades públicas responsables tienen derecho a negarse a proporcionar información a la persona interesada, o demorarse en proporcionarla;

c. el almacenamiento o destrucción de dichos datos.

Si una autoridad pública le indica a un operador de red o proveedor de servicios que efectúe una interferencia, los datos así recopilados deben comunicarse solo al organismo designado en la autorización de dicha injerencia".

4. Informe de 2015 de la Comisión Europea para la Democracia a través de la ley ("la Comisión de Venecia") sobre la supervisión democrática de las agencias de inteligencia de señales.

196. La Comisión de Venecia señaló, al principio, el valor que la interceptación masiva podía tener para las operaciones de seguridad, ya que habilitaba a los servicios de seguridad a adoptar un enfoque proactivo, buscando peligros hasta ahora desconocidos en lugar de investigar los conocidos. Sin embargo, también señaló que la interceptación masiva de datos en transmisión, o los requerimientos a las compañías de telecomunicaciones para que almacenaran y luego proporcionaran datos del contenido de las telecomunicaciones o metadatos a las fuerzas del orden o a las agencias de seguridad, implicaba una interferencia con la privacidad y otros derechos humanos de una gran proporción de la población del mundo. En este sentido, la Comisión de Venecia consideró que la principal interferencia con la privacidad ocurría cuando las agencias accedían y / o procesaban los datos personales almacenados. Por esta razón, el

análisis por ordenador (generalmente con la ayuda de selectores) era una de las etapas más importantes para equilibrar la integridad personal frente a otros intereses.

197. Según el informe, las dos salvaguardas más importantes eran la autorización (de obtención y acceso) y la fiscalización del proceso. De la jurisprudencia del Tribunal se desprende claramente que esta última debe ser realizada por un órgano externo e independiente. Si bien el Tribunal mostró su preferencia por la autorización judicial, no consideró que fuera un requisito necesario. Además, el sistema tenía que ser evaluado como un todo, y cuando los controles independientes estaban ausentes en la etapa de autorización, debían existir en la etapa de supervisión. En este sentido, la Comisión de Venecia consideró como ejemplo el sistema de los Estados Unidos, donde la autorización era otorgada por el FISC. Sin embargo, a pesar de la existencia de autorización judicial, la falta de supervisión independiente de las condiciones y las limitaciones impuestas por el Tribunal eran problemáticas.

198. Asimismo, la Comisión observó que la notificación al sujeto de la vigilancia no era un requisito absoluto del artículo 8 del Convenio, desde un procedimiento general de reclamación hasta un organismo de supervisión podían compensar la falta de notificación.

199. En el informe también se consideraba que los controles internos eran una "salvaguarda primaria". El reclutamiento y la formación eran cuestiones clave; además, era importante que las agencias desarrollasen el respeto a la privacidad y otros derechos humanos a la hora de promulgar normas internas.

200. El informe reconoció que los periodistas son un grupo que requiere de una protección especial, ya que la búsqueda de sus contactos podía revelar sus fuentes (y el riesgo de descubrimiento podía ser un poderoso desincentivo para denunciantes). Sin embargo, consideró que no existía una prohibición absoluta de registrar los contactos de los periodistas, siempre que hubiera razones muy poderosas para hacerlo. Según el informe, la profesión periodística no era fácil de identificar, ya que las ONGs también estaban comprometidas en la construcción de la opinión pública e incluso los blogueros podrían afirmar tener derecho a protecciones equivalentes.

201. Finalmente, el informe abordó brevemente el tema del intercambio de inteligencia, y en particular el riesgo de que los Estados de ese modo pudieran eludir procedimientos de vigilancia nacional más estrictos y / o cualquier límite legal al que sus agencias pudieran estar sujetas en lo que respecta a las operaciones nacionales de inteligencia. Consideró que una salvaguarda adecuada sería establecer que el material transferido de forma masiva solo podía ser registrado si se cumplieron los requisitos materiales de una búsqueda nacional y ésta era debidamente autorizada de la misma manera que una búsqueda de material masiva obtenida por las agencias de inteligencia de señales utilizando sus propias técnicas.

III.- NORMATIVA DE LA UNIÓN EUROPEA.

A. Carta de los Derechos Fundamentales de la Unión Europea.

202. Los artículos 7, 8 y 11 de la Carta establecen lo siguiente:

" **Artículo 7 Respeto de la vida privada y familiar**

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

Artículo 8 Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Artículo 11 Libertad de expresión y de información

1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.

2. Se respetan la libertad de los medios de comunicación y su pluralismo."

B. Directivas y otras normas de la Unión Europea relacionadas con la protección y el procesamiento de datos personales.

203. La Directiva de protección de datos (Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos), adoptada el 24 de octubre de 1995, ha regulado durante muchos años la protección y el tratamiento de datos personales dentro del Unión Europea. Como las actividades de los Estados Miembros en materia de seguridad pública, defensa y seguridad quedan fuera del ámbito de aplicación del Derecho comunitario la Directiva no se aplicó a estas actividades (artículo 3, apartado 2).

204. El Reglamento general de protección de datos, adoptado en abril de 2016, sustituyó a la Directiva de protección de datos y pasó a ser la norma aplicable a partir del 25 de mayo de 2018. El reglamento, que es directamente aplicable en los Estados Miembros[2], contiene disposiciones y requisitos relacionados con el procesamiento de información que permita la identificación personal de los interesados dentro de la Unión Europea, y se aplica a todas las empresas, independientemente de su ubicación, que hacen negocios con el Espacio Económico Europeo. Los procesos comerciales que manejan datos personales deben construirse con base protección de datos por diseño y por defecto, lo que significa que los datos personales deben almacenarse mediante seudonimización o anonimización y utilizarse la configuración de privacidad más alta posible de forma predeterminada, para que los datos no estén disponibles públicamente sin el consentimiento explícito, y que no permitan identificar a un sujeto sin una información adicional almacenada por separado. No se pueden procesar datos personales a menos que se haga conforme a una causa legal especificada en el reglamento, o si el controlador o procesador de datos ha recibido el consentimiento explícito y la aceptación del propietario de los datos. El propietario de los datos tiene derecho a revocar esta autorización en cualquier momento.

205. Un procesador de datos personales debe manifestar claramente cualquier recolección de datos, declarar la base legal para ello y el fin del procesamiento de datos,

[2] Antes de que el Reino Unido abandonara la Unión Europea, otorgó el consentimiento real a la Ley de Protección de datos de 23 de mayo de 2018, que contiene normas y protecciones equivalentes.

cómo se están reteniendo los datos a largo plazo, y si se están compartiendo con cualquier tercero o fuera de la Unión Europea. Los usuarios tienen derecho a solicitar una copia portátil de los datos recopilados por un procesador en un formato común, y el derecho a que se borren sus datos en determinadas circunstancias. Las autoridades públicas y empresas cuyas actividades principales se centran en el procesamiento regular o sistemático de datos personales, están obligados a contar con un delegado de protección de datos (DPO), que es responsable de gestionar el cumplimiento del RGPD. Las empresas deben informar sobre cualquier infracción en materia de datos en un plazo de 72 horas si tienen un efecto adverso sobre la privacidad del usuario.

206. La Directiva sobre privacidad y comunicaciones electrónicas (Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas), adoptada el 12 de julio de 2002, afirma, en los considerandos 2 y 11:

> "(2) La presente Directiva pretende garantizar el respeto de los derechos fundamentales y observa los principios consagrados, en particular, en la Carta de los Derechos Fundamentales de la Unión Europea. Señaladamente, la presente Directiva pretende garantizar el pleno respeto de los derechos enunciados en los artículos 7 y 8 de dicha Carta.
>
> ... ...
>
> (11) Al igual que la Directiva 95/46/CE, la presente Directiva no aborda la protección de los derechos y las libertades fundamentales en relación con las actividades no regidas por el Derecho comunitario. Por lo tanto, no altera el equilibrio actual entre el derecho de las personas a la intimidad y la posibilidad de que disponen los Estados miembros, según se indica en el apartado 1 del artículo 15 de la presente Directiva, de tomar las medidas necesarias para la protección de la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del Derecho penal. En consecuencia, la presente Directiva no afecta a la capacidad de los Estados miembros para interceptar legalmente las comunicaciones electrónicas o tomar otras medidas, cuando sea necesario, para cualquiera de estos fines y de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, según la interpretación que se hace de éste en las sentencias del Tribunal Europeo de Derechos Humanos. Dichas medidas deberán ser necesarias en una sociedad democrática y rigurosamente proporcionales al fin que se pretende alcanzar y deben estar sujetas, además, a salvaguardas adecuadas, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales"

207. La Directiva establece, asimismo, a los efectos que aquí nos interesan, que:

> "
>
> **Artículo 1 Ámbito de aplicación y objetivo**
>
> 1. La presente Directiva armoniza las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad.
>
> 2. Las disposiciones de la presente Directiva especifican y completan la Directiva 95/46/CE a los efectos mencionados en el apartado 1. Además, protegen los intereses legítimos de los abonados que sean personas jurídicas.
>
> 3. La presente Directiva no se aplicará a las actividades no comprendidas en el ámbito de aplicación del Tratado constitutivo de la Comunidad Europea, como las reguladas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea, ni, en cualquier caso, a las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado

(incluido el bienestar económico del Estado cuando dichas actividades estén relacionadas con la seguridad del mismo) y a las actividades del Estado en materia penal.

Artículo 15 Aplicación de determinadas disposiciones de la Directiva 95/46/CE

1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea. …"

208. El 15 de marzo de 2006, fue adoptada la Directiva de retención de datos (Directiva 2006/24/CE sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE). Antes de la sentencia de 2014 declarándola inválida (ver párrafo 209 siguiente), disponía, a los efectos que aquí nos conciernen:

Artículo 1 Objeto y ámbito

1. La presente Directiva se propone armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro.

2. La presente Directiva se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas.

Artículo 3 Obligación de conservar datos

1. Como excepción a los artículos 5, 6 y 9 de la Directiva 2002/58/CE, los Estados miembros adoptarán medidas para garantizar que los datos especificados en el artículo 5 de la presente Directiva se conservan de conformidad con lo dispuesto en ella en la medida en que son generados o tratados por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo su jurisdicción en el marco de la prestación de los servicios de comunicaciones de que se trate…."

C. Jurisprudencia relevante del Tribunal de Justicia de la Unión Europea ("TJUE")

1. Digital Rights Ireland Ltd contra el Ministro de Comunicaciones, Marina y Recursos naturales y otros y Kärntner Landesregierung y Otros (asuntos C-293/12 y C-594/12; ECLI:EU C:2014:238)

209. En su sentencia de 8 de abril de 2014, el TJUE declaró inválida la Directiva 2006/24/CE de conservación de datos por la que se establecía la obligación de los proveedores de servicios de comunicaciones electrónicas disponibles al público o de

redes de comunicaciones públicas de conservar todos los datos del tráfico y de ubicación por períodos de seis meses a dos años, con el fin de garantizar que los datos estarían disponible a los efectos de la investigación, detección y enjuiciamiento de delitos graves, según la definición de cada Estado Miembro en su legislación nacional. El TJUE señaló que, aunque la directiva no permitía la retención del contenido de la comunicación, los datos del tráfico y de ubicación permitían extraer conclusiones muy precisas sobre las vidas de las personas cuyos datos se habían conservado. En consecuencia, la obligación de conservar los datos constituía en sí misma una injerencia en el derecho al respeto de la vida privada y las comunicaciones garantizado por el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea y el derecho a la protección de datos personales en virtud del artículo 8 de la Carta.

210. El acceso de las autoridades nacionales competentes a los datos constituía una injerencia en esos derechos fundamentales, que el TJUE consideró "particularmente grave". El hecho de que los datos fueran conservados y posteriormente utilizados sin que el suscriptor o usuario registrado fueran informados hacía, según el TJUE, probable que generara en las mentes de las personas afectadas el sentimiento de que su vida privada era objeto de una vigilancia constante. La injerencia satisfacía un objetivo de interés general, a saber, contribuir a la lucha contra la delincuencia grave y el terrorismo y así, en última instancia, a la seguridad pública. Sin embargo, no cumplía el requisito de proporcionalidad.

211. En primer lugar, la Directiva abarcaba, de manera generalizada, a todas las personas y todos los medios de comunicación electrónicos, así como todos los datos del tráfico sin distinción alguna, limitación o excepción en función del objetivo de la lucha contra la delincuencia grave. Por tanto, implicaba una injerencia en los derechos fundamentales de prácticamente toda la población de los países europeos, según el TJUE. Se aplicaba incluso a personas sobre las que no había evidencias que sugirieran que su conducta pudiera tener un vínculo, incluso indirecto o remoto, con un delito grave.

212. En segundo lugar, la Directiva no regulaba aspectos sustantivos ni procedimentales acerca de las condiciones relativas al acceso por las autoridades nacionales competentes a los datos y su posterior uso. Simplemente hacía referencia, de manera general, a delitos graves, según la definición de cada Estado Miembro en su legislación nacional, la Directiva no estableció ningún criterio objetivo para determinar qué delitos podían considerarse suficientemente graves para justificar tan amplia injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta. Sobre todo, el acceso por parte de las autoridades nacionales competentes a los datos conservados no se hizo depender de una revisión previa llevada a cabo por un tribunal o por un organismo administrativo independiente cuya decisión limitara el acceso a los datos y su uso a aquellos supuestos en los que fuera estrictamente necesario para la consecución del objetivo perseguido.

213. En tercer lugar, la Directiva exigía que todos los datos se conservaran durante un período de al menos seis meses, sin que se hiciera distinción entre las categorías de datos sobre la base de su posible utilidad para los objetivos perseguidos o según las personas a las que afectaba. El TJUE llegó a la conclusión de que la Directiva entrañaba una amplia y especialmente grave injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, sin que tal injerencia estuviese circunscrita de forma

precisa por disposiciones para garantizar que en la práctica se limitara a los supuestos en los que fuera a estrictamente necesario. El TJUE también señaló que la Directiva no preveía suficientes salvaguardas, mediante medidas técnicas y organizativas, para garantizar una protección eficaz de los datos conservados contra el riesgo de abuso y contra cualquier acceso y uso ilícitos de esos datos.

2. Tele2 Sverige AB c. Post- och telestyrelsen y el Ministro de Interior contra Tom Watson y otros (casos C-203/15 y C-698/15; ECLI:UE:C:2016:970)

214. En el asunto *Ministro de Interior c. Watson y Otros*, los demandantes habían solicitado la revisión judicial de la legalidad del artículo 1 de la Ley de retención de datos y poderes de investigación de 2014 ("DRIPA"- siglas en inglés-), conforme al cual el Secretario de Estado podía requerir a un operador de telecomunicaciones que retuviera datos de comunicaciones relevantes si lo consideraba necesario y proporcionado para uno o más de los fines previstos en los párrafos (a) a (h) de la sección 22 (2) de la RIPA. Los demandantes alegaron, entre otras cuestiones, que la sección 1 era incompatible con artículos 7 y 8 de la Carta y el artículo 8 del Convenio.

215. El 17 de julio de 2015, el Tribunal Superior dictaminó que la sentencia *Derechos Digitales* establecía los "requisitos obligatorios de la legislación de la UE" aplicables a la legislación de los Estados Miembros sobre la conservación de datos relacionados con las comunicaciones y el acceso a dichos datos. Dado que el TJUE, en dicha sentencia, sostuvo que la Directiva 2006/24 era incompatible con el principio de proporcionalidad la legislación nacional que contuviera las mismas disposiciones que dicha directiva podía, igualmente, no ser compatible con ese principio. De hecho, se desprende de la lógica subyacente de la sentencia de *Derechos Digitales* que la legislación que estableciera un cuerpo general de reglas para la retención de datos de las comunicaciones violaba los derechos garantizados en los artículos 7 y 8 de la Carta, a menos que esa legislación se complementara con un conjunto de normas para el acceso a los datos, previstas por la legislación nacional, que ofrecieran garantías suficientes para proteger esos derechos. En consecuencia, la sección 1 de la DRIPA no era compatible con los artículos 7 y 8 de la Carta, ya que no establecía de manera clara y precisa las reglas que permiten el acceso y uso de los datos retenidos y el acceso a aquellos datos no se hacía depender de una revisión previa por parte de un tribunal o un organismo administrativo independiente.

216. Presentada apelación por el Secretario de Estado, el Tribunal de Apelación planteó una cuestión prejudicial al TJUE.

217. Ante el TJUE este caso fue acumulado a la cuestión prejudicial planteada por Kammarrätten i Stockholm en el asunto C-203/15 *Tele2 Sverige AB contra Post- och telestyrelsen*. Tras una vista oral en la que intervinieron unos quince Estados Miembros de la Unión Europea, el TJUE dictó sentencia el 21 de diciembre de 2016. El TJUE sostuvo que el artículo 15, apartado 1, de la Directiva 2002/58, interpretada a la luz de los artículos 7, 8 y 11 y el artículo 52, apartado 1 de la Carta, debía interpretarse en el sentido de que se oponía a la legislación nacional que rige la protección y seguridad del tráfico y los datos de ubicación y, en particular, el acceso de las autoridades nacionales competentes a los datos conservados, cuando el objetivo perseguido por dicho acceso, en el contexto de la lucha contra la delincuencia, no se restringía únicamente a la lucha contra la delincuencia grave, cuando el acceso no estaba sujeto a revisión previa por un

tribunal o una autoridad administrativa independiente, y cuando no había ningún requisito de que los datos en cuestión debieran mantenerse dentro de la Unión Europea.

218. El TJUE declaró la cuestión planteada por el Tribunal de Apelación de si la protección otorgada por los artículos 7 y 8 de la Carta era más amplia que la garantizada por el artículo 8 del Convenio inadmisible.

219. Tras dictarse sentencia por el TJUE, el caso fue devuelto al Tribunal de Apelación. El 31 de enero de 2018 dictó una resolución declarativa en los siguientes términos: que el artículo 1 de la DRIPA era incompatible con la legislación de la Unión Europea en la medida en que permitía el acceso a los datos conservados pese a que el objeto perseguido por el acceso no se restringía únicamente a la lucha contra la delincuencia grave; o aun cuando el acceso no estaba sujeto a revisión previa por un tribunal o una autoridad administrativa independiente.

3. Ministerio Fiscal (Asunto C-207/16; ECLI:EU:C:2018:788)

220. Esta cuestión prejudicial se planteó con posterioridad a que la policía española, en el curso de una investigación sobre el robo de una cartera y un teléfono móvil, pidiera al juez de instrucción que les autorizara el acceso a los datos que identificaran a los usuarios de los números de teléfonos activados con el teléfono robado durante un período de doce días antes del robo. El juez de instrucción rechazó la solicitud basándose, entre otras cuestiones, en que los hechos que dieron lugar a la investigación criminal no constituían un delito "grave". Posteriormente, el referido juzgado, solicitó orientación al TJUE para la fijación del umbral de gravedad de las infracciones por encima del cual una injerencia en derechos fundamentales, como el acceso de las autoridades nacionales competentes a los datos personales a través de proveedores de servicios de comunicaciones electrónicas, pudiera estar justificado.

221. El 2 de octubre de 2018, la Gran Sala del TJUE dictaminó que el artículo 15, apartado 1, de la Directiva 2002/58/CE, leído a la luz de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, tenía que ser interpretado en el sentido de que debe interpretarse en el sentido de que el acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares, constituye una injerencia en los derechos fundamentales de éstos, consagrados en los citados artículos de la Carta de los Derechos Fundamentales, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave. En particular, indicó que:

> "…conforme al principio de proporcionalidad, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos solo puede justificar una injerencia grave el objetivo de luchar contra la delincuencia que a su vez esté también calificada de «grave».
>
> En cambio, cuando la injerencia que implica dicho acceso no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general.".

222. No consideró que el acceso a los datos objeto de la solicitud constituyera una interferencia particularmente grave porque:

> "Solo permiten vincular, durante un período determinado, la tarjeta o tarjetas SIM activadas con el teléfono móvil sustraído y los datos personales o de filiación de los titulares de estas tarjetas

SIM. Sin un cotejo con los datos relativos a las comunicaciones realizadas con esas tarjetas SIM y de localización, estos datos no permiten conocer la fecha, la hora, la duración o los destinatarios de las comunicaciones efectuadas con las tarjetas SIM en cuestión, ni los lugares en que estas comunicaciones tuvieron lugar, ni la frecuencia de estas con determinadas personas durante un período concreto. Por tanto, dichos datos no permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados.".

4. Maximillian Schrems c. Comisionado de Protección de Datos (Asunto C-362/14; ECLI: EU: C: 2015: 650)

223. Esta cuestión prejudicial se planteó a raíz de una reclamación contra Facebook Ireland Ltd, que se hizo al Comisionado de protección de datos irlandés por el Sr. Schrems, un defensor de la privacidad de Austria. El Sr. Schrems impugnó la transferencia de sus datos por parte de Facebook Irlanda a los Estados Unidos y la conservación de sus datos en servidores ubicados en ese país. El Comisionado de protección de datos rechazó la reclamación ya que, en una decisión del 26 de julio de 2000, la Comisión Europea había considerado que los Estados Unidos aseguraban un nivel adecuado de protección de los datos personales transferidos ("la Decisión de puerto seguro").

224. En su sentencia de 6 de octubre de 2015, el TJUE sostuvo que la existencia de una decisión de la Comisión determinando que un tercer país garantiza un adecuado nivel de protección de los datos personales transferidos no puede eliminar ni reducir las facultades de las autoridades nacionales de supervisión en virtud de la Carta o de la Directiva de protección de datos. Por lo tanto, incluso si la Comisión había adoptado una decisión, las autoridades nacionales de supervisión tenían la capacidad de examinar, con total independencia, si la transferencia de los datos de una persona a un tercer país cumplía con los requisitos establecido por la Directiva.

225. Sin embargo, solo el TJUE podía declarar una decisión de la Comisión inválida. A este respecto, señaló que la Decisión de puerto seguro era aplicable únicamente a las entidades de los Estados Unidos que se adhirieron a él, y las autoridades públicas de los Estados Unidos no estaban sujetas a él. Además, la seguridad nacional, el interés público y la aplicación de los requisitos legales de los Estados Unidos prevalecían sobre el sistema de puerto seguro, de modo que las entidades de los Estados Unidos estaban obligadas a hacer caso omiso, sin limitación, de las normas de protección establecidas por el sistema cuando entraban en conflicto con tales requisitos. Por tanto, la Decisión puerto seguro permitía la interferencia de las autoridades públicas de los Estados Unidos en los derechos fundamentales de las personas, y la Comisión, no se había referido, en la Decisión puerto seguro, a la existencia, en los Estados Unidos, de reglas destinadas a limitar dicha interferencia, o a la existencia de protección legal contra la injerencia.

226. En cuanto a si el nivel de protección en los Estados Unidos era esencialmente equivalente a los derechos y libertades fundamentales garantizados dentro de la Unión Europea, el TJUE concluyó que la legislación no limitaba la autorización a lo estrictamente necesario, de forma generalizada, el almacenamiento de todos los datos personales de todas las personas cuyos datos fueron transferidos de la Unión Europea a los Estados Unidos sin ninguna diferenciación, limitación o excepción a la luz del objetivo perseguido y sin que se estableciera un criterio objetivo para determinar los límites del acceso de las autoridades públicas a los datos y su uso posterior. Por lo tanto,

según la legislación de la Unión Europea permitir a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas debía considerarse una conducta comprometedora de la esencia del derecho fundamental al respeto de la vida privada. Igualmente, la legislación que no preveía ninguna posibilidad para que un individuo ejercitara acciones legales o recursos para tener acceso a los datos personales que le conciernen, o para obtener la rectificación o supresión de dichos datos, comprometiendo la esencia del derecho fundamental a la tutela judicial efectiva.

227. Finalmente, el Tribunal concluyó que la Decisión puerto seguro denegaba a las autoridades nacionales sus poderes de supervisión cuando una persona cuestionaba si la decisión era compatible con la protección de la privacidad y de los derechos y libertades fundamentales de las personas. La Comisión no tenía competencias para restringir los poderes de supervisión de las autoridades nacionales de esa manera y, en consecuencia, el TJUE sostuvo que la Decisión puerto seguro era inválida.

5. El asunto del Comisionado de Protección de Datos contra Facebook Irlanda y Maximillian Schrems (C-311/18; ECLI: EU: C: 2020: 559)

228. Siguiendo lo establecido en la sentencia del TJUE de 6 de octubre de 2015, el tribunal remitente anuló el rechazo de la reclamación del Sr. Schrems y remitió esa decisión de nuevo al Comisionado. En el transcurso de la investigación del Comisionado, Facebook Irlanda explicó que una gran parte de datos personales se transfirieron a Facebook Inc. de conformidad con las cláusulas estándar de protección de datos establecidas en el anexo de la Decisión de la Comisión 2010/87 / UE, conforme fue modificada.

229. El Sr. Schrems reformuló su reclamación alegando, entre otras cuestiones, que la ley de los Estados Unidos requería a Facebook Inc. que los datos personales a él transferidos estuvieran disponibles para ciertas autoridades de los Estados Unidos, como la NSA y la Oficina Federal de Investigaciones. Dado que esos datos se utilizaron en el contexto de varios programas de seguimiento de una manera incompatible con los artículos 7, 8 y 47 de la Carta, la Decisión 2010/87 / UE no podía justificar la transferencia de esos datos a los Estados Unidos. Sobre esta base, solicitó al Comisionado que prohibiera o suspendiera la transferencia de sus datos personales a Facebook Inc.

230. En el proyecto de decisión publicado el 24 de mayo de 2016, el Comisionado adoptó el criterio provisional de que los datos personales de los ciudadanos de la Unión Europea transferidos a los Estados Unidos probablemente serían consultados y procesados por las autoridades de los Estados Unidos de forma incompatible con los artículos 7 y 8 de la Carta y que la ley de los Estados Unidos no preveía para esos ciudadanos acciones legales compatibles con el artículo 47 de la Carta. El Comisionado consideró que las cláusulas estándar de protección de datos del anexo de la Decisión 2010/87/UE no subsanaban ese defecto, ya que no obligaban a las autoridades de los Estados Unidos.

231. Habiendo considerado las actividades de inteligencia de los Estados Unidos bajo la sección 702 de la FISA y la Orden Ejecutiva 12333, el Tribunal Superior concluyó que los Estados Unidos habían llevado a cabo un procesamiento masivo de datos personales sin garantizar un nivel de protección esencialmente equivalente al garantizado por los artículos 7 y 8 de la Carta; y que los ciudadanos de la Unión Europea no tenían a su

disposición las mismas acciones legales que los ciudadanos de los Estados Unidos, con la consecuencia de que la ley de los Estados Unidos no concedía a los ciudadanos de la Unión Europea un nivel de protección esencialmente equivalente al garantizado por artículo 47 de la Carta. El Tribunal suspendió el procedimiento y remitió una serie de preguntas al TJUE a través de una cuestión prejudicial. Preguntó, entre otras cuestiones, si el Derecho de la Unión Europea es de aplicación a la cesión de datos de una empresa privada en la Unión Europea a una empresa privada en un tercer país; y de ser así, cómo debía evaluarse el nivel de protección en el tercer país; y si el nivel de protección otorgado por los Estados Unidos respetaba la esencia de los derechos garantizados por el artículo 47 de la Carta.

232. En la sentencia de 16 de julio de 2020, el TJUE sostuvo que el Reglamento general de protección de datos ("RGPD") se aplicaba a la transferencia de datos personales para fines comerciales por un operador económico establecido en un Estado Miembro a otro operador económico establecido en un tercer país, independientemente de si, en el momento de dicha transferencia o posteriormente, esos datos podían ser procesados por las autoridades del tercer país en cuestión a los efectos de seguridad pública, defensa y seguridad del Estado. Además, las salvaguardas adecuadas, los derechos exigibles y los recursos legales requeridos por el RGPD tenían que garantizar que los interesados cuyos datos personales se transfirieron a un tercer país de conformidad con las cláusulas estándar de protección de datos recibían un nivel de protección esencialmente equivalente al garantizado dentro de la Unión Europea. Con ese fin, la evaluación del nivel de protección otorgado en el contexto de dicha transferencia tenía que tener en cuenta tanto las cláusulas contractuales pactadas entre los responsables o encargados del tratamiento en la Unión Europea y el destinatario de la transferencia del país tercero de que se trate y, en lo que respecta a cualquier acceso de las autoridades públicas de ese tercer país a los datos personales transferidos, los aspectos pertinentes del sistema legal de ese tercer país.

233. Además, a menos que hubiera una decisión válida de adecuación de la Comisión, la autoridad de control competente estaba obligada a suspender o prohibir una transferencia de datos a un tercer país si, a juicio de esa autoridad supervisora y a la luz de todas las circunstancias de esa transferencia, las cláusulas estándar de protección de datos adoptadas por la Comisión no se cumplieran o no pudieran cumplirse en ese tercer país y la protección de los datos transferidos (tal y como requiere la ley de la Unión Europea) no pudiera garantizarse por otros medios.

234. Para que la Comisión adoptara una decisión de adecuación, había de constatar, mediante razones debidamente motivadas, que el tercer país de que se tratara asegurara, en razón de su derecho interno o de sus compromisos internacionales, un nivel de protección de los derechos fundamentales esencialmente equivalente al garantizado en el ordenamiento jurídico de la Unión Europea. En opinión del TJUE, la Decisión Puerto Seguro era inválida. La sección 702 de la Ley de Seguridad de Inteligencia Extranjera ("FISA"- siglas en inglés-) no establecía ninguna limitación al poder que confería para implementar programas de vigilancia con fines de inteligencia extranjera ni establecía garantías para las personas no estadounidenses potencialmente objetivo de esos programas. En esas circunstancias, no podía garantizar un nivel de protección esencialmente equivalente al garantizado por la Carta. Además, en lo que respecta a los programas de seguimiento basados en la Orden Ejecutiva 12333, era claro que esa orden

tampoco confería derechos que fueran ejercitables frente las autoridades de los Estados Unidos ante los tribunales.

6. Privacidad Internacional contra el Secretario de Estado de Relaciones Exteriores y Asuntos de la Mancomunidad de Naciones y otros (asunto C-623/17;ECLI:EU:C:2020:790) y La Quadrature du Net y otros, French Data Network y otros y Ordre des barreaux francófonos y germanófonos y otros (asuntos C-511/18, C-512/18 y C-520/18; ECLI:UE:C:2020:791)

235. El 8 de septiembre de 2017, el IPT dictó sentencia en el caso *Privacidad Internacional*, que versaba sobre la adquisición masiva por parte de los servicios de inteligencia de datos de comunicaciones bajo la sección 94 de la Ley de Telecomunicaciones de 1984 y de datos personales. El IPT consideró que, siguiendo su declaración, los regímenes cumplían con el artículo 8 del Convenio. Sin embargo, identificó los siguientes cuatro requisitos que parecían derivar de la sentencia del TJUE en el asunto *Watson y otros* y que parecían ir más allá de los requisitos del artículo 8 del Convenio: la restricción del acceso no dirigido a datos masivos; la necesidad de autorización previa (salvo en casos de emergencia válidamente acreditados) antes de que pueda accederse a los datos; la notificación posterior a los afectados; y la retención de todos los datos dentro de la Unión Europea.

236. El 30 de octubre de 2017, el IPT planteó al TJUE una cuestión prejudicial para que aclarara en qué medida los requisitos del asunto *Watson* podían aplicarse a la adquisición masiva y a las técnicas de procesamiento automatizado cuando eran necesarias para proteger la seguridad nacional. Al hacerlo, expresó su grave preocupación de que, si los requisitos del asunto *Watson* se aplicaran a medidas tomadas para salvaguardar la seguridad nacional, las frustrarían y pondrían en peligro la seguridad nacional de los Estados Miembros. En particular, señaló los beneficios de la adquisición masiva en el contexto de la seguridad nacional; el riesgo de que la necesidad de autorización previa pudiera socavar la capacidad de los servicios de inteligencia para hacer frente a las amenazas a la seguridad nacional; el peligro y la impracticabilidad de implementar un requisito de notificar la adquisición o uso de una base de datos masivos, especialmente cuando la seguridad nacional estaba en juego; y el impacto que una barrera absoluta en la transferencia de datos fuera de la Unión Europea podría tener sobre las obligaciones de los Estados Miembros en virtud de los tratados.

237. El 9 de septiembre de 2019 tuvo lugar una vista pública. El asunto *Privacidad Internacional* fue tramitado junto con los asuntos C-511/18 y C-512/18, *La Quadrature du Net y otros*, y C-520/18, *Ordre des barreaux francófonos y germanófonos y otros*, que también se referían a la aplicación de la Directiva 2002/58 a las actividades relacionadas con la seguridad nacional y la lucha contra el terrorismo. Trece Estados intervinieron en apoyo de los Estados interesados.

238. El 6 de octubre de 2020 se dictaron dos sentencias distintas. En el asunto *Privacidad Internacional*, el TJUE consideró que la legislación nacional que permitía a la autoridad del Estado exigir a los proveedores de servicios de comunicaciones electrónicas que les reenviaran datos de tráfico y datos de ubicación a las agencias de seguridad e inteligencia con el fin de salvaguardar la seguridad nacional entraban dentro del ámbito de aplicación de la Directiva sobre privacidad y comunicaciones electrónicas. La interpretación de dicha Directiva debía tener en cuenta el derecho a la

intimidad garantizado por el artículo 7 de la Carta, el derecho a la protección de datos, garantizado por el artículo 8, y el derecho a la libertad de expresión, garantizado por el artículo 11. Las limitaciones al ejercicio de esos derechos tenían que estar previstas en la ley, respetar el núcleo esencial de dichos derechos y ser proporcionadas, necesarias y que realmente cumplieran con los objetivos de interés general reconocidos por la Unión Europea o con la necesidad de proteger los derechos y libertades de terceros. Además, las limitaciones a la protección de los datos personales deben aplicarse solo en la medida en que sean estrictamente necesarias; y, en orden a satisfacer el requisito de proporcionalidad, la legislación debe establecer reglas claras y precisas que rijan el alcance y la aplicación de la medida de que se trate imponiendo garantías mínimas, para que las personas cuyos datos personales están afectados tengan garantías suficientes de que los datos serán protegidos eficazmente contra el riesgo de abuso.

239. En opinión del TJUE, la legislación nacional que exige a los proveedores de servicios de comunicaciones electrónicas divulgar datos del tráfico y datos de ubicación a las agencias de seguridad e inteligencia mediante una transmisión general e indiscriminada - la cual afectó a todas las personas que utilizaran servicios de comunicaciones – excedía de los límites de lo que era estrictamente necesario y no podía considerarse justificada conforme requiere la Directiva sobre privacidad y comunicaciones electrónicas interpretada a la luz de la Carta.

240. Sin embargo, en el asunto *La Quadrature du Net y otros*, el TJUE confirmó que si bien la Directiva sobre privacidad y comunicaciones, interpretada a la luz de la Carta, excluía medidas legislativas que previeran la retención general e indiscriminada de datos del tráfico y datos de ubicación, cuando un Estado Miembro se enfrentaba a una grave amenaza para la seguridad que fuera genuina y presente o previsible, no se excluían medidas legislativas que requirieran que los proveedores de servicios retuvieran, de forma general e indiscriminada, los datos de tráfico y ubicación durante un período de tiempo limitado a lo que fuera estrictamente necesario, el cual podía ampliarse si persistía la amenaza. Con el fin de combatir delitos graves y prevenir amenazas graves a la seguridad pública, un Estado Miembro también podía solicitar, siempre que estuviera limitado en el tiempo hasta cuando fuera estrictamente necesario: la retención específica de datos del tráfico y datos de ubicación, sobre la base de factores objetivos y no discriminatorios según las categorías de personas de interés o utilizando un criterio geográfico, o direcciones IP asignadas a la fuente de una conexión a Internet. También estaba abierto a que un Estado Miembro llevara a cabo una acción general e indiscriminada de retención de datos relacionados con la identidad civil de los usuarios de medios de comunicación electrónicos, sin que la retención estuviera sujeta a un límite de tiempo específico.

241. Además, la Directiva sobre privacidad y comunicaciones, leída a la luz de la Carta, no excluía las normas nacionales que exigieran a los proveedores de servicios de comunicaciones electrónicas recurrir, en primer lugar, al análisis automatizado y la recopilación de datos del tráfico y datos de ubicación en tiempo real, y en segundo lugar, a la recopilación en tiempo real de datos técnicos relativos a la ubicación del equipo terminal utilizado, los que estaba limitado a aquellas situaciones en las que un Estado Miembro se enfrentaba a una grave amenaza para la seguridad nacional que fuera genuina y presente o previsible, y cuando el recurso a dicho análisis pudiera ser objeto de una revisión eficaz por parte de un tribunal u organismo administrativo independiente cuya decisión fuera vinculante; y cuando se recurría a la recopilación en

tiempo real de datos de tráfico y ubicación limitados a personas respecto de las cuales había una razón válida para sospechar que estaban involucrados en actividades terroristas y estaba sujeto a una revisión previa realizada por un tribunal o por un organismo administrativo independiente cuya decisión fuera vinculante.

IV. DERECHO COMPARADO Y COSTUMBRE

A. Estados contratantes

242. Al menos siete Estados contratantes (Finlandia, Francia, Alemania, los Países Bajos, Suecia, Suiza y el Reino Unido) utilizan oficialmente regímenes de interceptación masiva a través de cables y por vía aérea.

243. En otro Estado (Noruega) se está debatiendo un proyecto de ley: que, si es aprobado, también autorizará la interceptación masiva.

244. Los detalles del sistema sueco pueden encontrarse en la sentencia del asunto *Centrum för rättvisa c. Suecia* (demanda núm. 35252/08); y los detalles del sistema alemán se exponen en los párrafos 247-252 siguientes.

245. En lo que respecta a los acuerdos de intercambio de inteligencia, al menos treinta y nueve de los Estados contratantes han celebrado acuerdos de intercambio de inteligencia con otros Estados, o existe la posibilidad de que suscriban tales acuerdos. Dos prohíben expresamente y dos permiten expresamente que el Estado solicite a una potencia extranjera la interceptación de material en su nombre. En los Estados restantes, la posición sobre este asunto no es clara.

246. Por último, en la mayoría de los Estados las salvaguardas aplicables son, en general, las mismas que para las operaciones internas, con varias restricciones en el uso de los datos recibidos y, en algunos casos, con la obligación de destruirlos si devienen irrelevantes.

B. Sentencia del Tribunal Constitucional Federal de Alemania de 19 de mayo 2020 (1 BvR 2835/17)

247. En esta sentencia, el Tribunal Constitucional evaluó si los poderes del Servicio Federal de Inteligencia para llevar a cabo estrategias (o “señales”) de inteligencia sobre telecomunicaciones extranjeras violaban los derechos fundamentales contenidos en la Ley Fundamental (*Grundgesetz*).

248. El régimen en cuestión implicaba la interceptación tanto de contenidos como de datos de comunicaciones y tenía como finalidad monitorear únicamente telecomunicaciones fuera del territorio alemán. Tal vigilancia podía ser realizada con el fin de obtener información sobre determinados temas que por mandato del Gobierno Federal pudieran ser relevantes para la política exterior y de seguridad del Estado. Sin embargo, también podía usarse para vigilar a individuos específicos. La admisibilidad y necesidad de las órdenes para realizar tal vigilancia era controlada por un grupo de expertos independientes. De acuerdo con la sentencia del Tribunal Constitucional, a la interceptación le seguía un proceso de filtrado y evaluación totalmente automatizado de varias etapas. Para este fin, el Servicio Federal de Inteligencia usaba un número de seis dígitos de términos de búsqueda que estaban sujetos al control de una subunidad interna responsable de garantizar que el vínculo entre los términos de búsqueda empleados y el

fin de la solicitud de los datos se motivaba de manera razonable y completa. Tras la aplicación del proceso automatizado de filtrado, el material interceptado era eliminado o almacenado y enviado para su evaluación por un analista.

249. El intercambio de material interceptado con servicios de inteligencia extranjeros iba acompañado de un acuerdo de cooperación que debía incluir la aplicación de restricciones y garantías para asegurar que los datos se manejaran y eliminaran de conformidad con los principios del estado de derecho.

250. El Tribunal Constitucional sostuvo que el régimen en cuestión no era conforme a la Ley Fundamental. Si bien reconoció el interés público predominante en la recopilación efectiva de inteligencia extranjera, no obstante consideró, entre otras cuestiones, que el régimen no estaba restringido a fines lo suficientemente específicos; no estaba estructurado de una manera que permitiera una adecuada supervisión y control; y faltaban varias salvaguardas, en particular con respecto a la protección de periodistas, abogados y otras personas cuyas comunicaciones requerían una protección especial respecto a su confidencialidad.

251. Con respecto al intercambio de información de inteligencia obtenida a través de vigilancia extranjera, el Tribunal consideró igualmente que faltaban salvaguardas. En particular, no se especificaba con suficiente claridad cuando intereses de peso podían justificar la transferencia de datos. Además, aunque el Tribunal no consideró necesario que un Estado receptor tuviera normas comparables sobre el tratamiento de datos personales, consideró, no obstante, que los datos solo podían transferirse al extranjero si existía un nivel adecuado de protección de los datos y no existían motivos para temer que la información se utilizara para violar los principios del estado de derecho. De manera más general, en el contexto del intercambio de inteligencia, el tribunal consideró que la cooperación con Estados extranjeros no debería ser utilizada para socavar las salvaguardas nacionales y si el Servicio Federal de Inteligencia deseaba utilizar los términos de búsqueda que le proporcionaba un servicio de inteligencia extranjero, primero debía confirmar la existencia del vínculo necesario entre los términos de búsqueda y el fin de la solicitud de datos y que los datos resultantes no revelaran una necesidad particular de confidencialidad (por ejemplo, porque se refirieran a denunciantes o disidentes). Aunque el Tribunal no excluyó la posibilidad de transferencia masiva de datos a servicios de inteligencia extranjeros, consideró que no podía ser un proceso continuo basado en un único fin.

252. Finalmente, el Tribunal determinó que las facultades de vigilancia que estaban siendo objeto de revisión carecían también de una amplia supervisión independiente y continua que sirviera para velar por el cumplimiento de la ley y compensar la potencial ausencia de salvaguardas comúnmente garantizadas por el estado de derecho. El legislador tenía que prever dos tipos diferentes de supervisión, que también tenían que ser reflejadas en el marco organizativo: en primer lugar, mediante un organismo parecido a un tribunal, encargado de realizar la supervisión y de decidir en un procedimiento formal proporcionar protección jurídica *ex ante* o *ex post*; y en segundo lugar, mediante una vigilancia de naturaleza administrativa que pudiera, por iniciativa propia, escudriñar aleatoriamente todo el procedimiento de vigilancia estratégica en cuanto a su legalidad. En opinión del Tribunal Constitucional, los pasos procesales clave serían, al menos, requerir la autorización *ex ante* de un organismo parecido a un tribunal, en concreto: la determinación formal de las diversas medidas de vigilancia (no

se descartaban las exenciones en casos de urgencia); el uso de los términos de búsqueda, en la medida en que los individuos a los que se dirigían de forma directa podían representar un peligro y, por lo tanto, eran de interés directo para el Servicio Federal de Inteligencia; el uso de términos de búsqueda dirigidos directamente a personas cuyas comunicaciones requerían una protección especial de confidencialidad; y cuando se fueran a compartir con servicios de inteligencia extranjeros datos de periodistas, abogados y otras profesiones que merezcan una especial protección respecto a su confidencialidad.

C. Sentencia del Tribunal de Apelación de La Haya de 14 de marzo de 2017

253. Varias personas y asociaciones alegaron que los servicios neerlandeses de inteligencia y seguridad actuaban ilegalmente al recibir datos de servicios de inteligencia y seguridad extranjeros, en particular de la NSA y de la GCHQ, los cuales en su opinión habían obtenido o podían haber obtenido los datos de forma "no autorizada" o "ilegal". Los demandantes no alegaron que las actividades de la NSA y la GCHQ eran "contrarias a la ley" o "ilegales" conforme al derecho interno, sino que la NSA había actuado violando el Pacto Internacional de Derechos Civiles y Políticos ("PIDCP") y la GCHQ había actuado violando el Convenio. Los demandantes se basaron, *inter alia*, en las "revelaciones de Snowden" (ver párrafo 12 anterior).

254. Las reclamaciones de los demandantes fueron desestimadas por el Tribunal de La Haya el 23 de julio de 2014 (ECLI:NL:RBDHA:2014:8966). El recurso de apelación frente a dicha sentencia fue desestimado por el Tribunal de Apelación de La Haya el 14 de marzo 2017 (ECLI:NL:GHDHA:2017:535).

255. El Tribunal de Apelación sostuvo que en principio había que confiar en que los Estados Unidos y Reino Unido cumplían con sus obligaciones en virtud de los tratados. Esa confianza solo podía ceder si salían a la luz circunstancias suficientemente concretas para suponer que estaba justificado.

256. Con respecto a la recopilación de datos de telecomunicaciones por parte de la NSA, no había indicios claros de que la NSA hubiera actuado en violación del Pacto Internacional de Derechos Civiles y Políticos. En la medida en que los demandantes habían tratado de argumentar que los poderes legales que sustentan la recopilación de datos eran más amplios de los permitidos bajo el Pacto Internacional de Derechos Civiles y Políticos, no habían explicado suficientemente respecto a qué leyes y reglamentos aplicables eran inadecuados.

257. Con respecto a la recopilación de datos por parte de la GCHQ, los demandantes no fundamentaron de manera alguna que la GCHQ estuviera actuando contraviniendo el Convenio.

258. Por lo tanto, los demandantes no lograron demostrar que la manera en que operaban la NSA y la GCHQ estaba, al menos en principio, en conflicto con el Pacto Internacional de Derechos Civiles y Políticos y el Convenio. Si bien no podía excluirse que en algún caso específico, la NSA o la GCHQ, o cualquier otro servicio de inteligencia extranjero, pudiera haber recopilado datos de una manera que violara el PIDCP o el Convenio, el principio de confianza impedía considerar que esta mera posibilidad implicaba que los servicios de inteligencia holandeses no pudieran recibir

datos de servicios de inteligencia extranjeros sin verificar en cada caso individual que estos datos se habían obtenido sin violar las obligaciones del tratado pertinente.

259. Finalmente, el Tribunal de Apelación admitió que, aunque los servicios de inteligencia extranjeros actuaron dentro de los límites de sus poderes legales y de las obligaciones previstas en los tratados, el hecho de que estos poderes legales pudieran ser más amplios que los de los servicios de inteligencia holandeses podía, en determinadas circunstancias, plantear problemas. Por ejemplo, era posible que los servicios de inteligencia holandeses estuvieran actuando en contra de la Ley de Servicios de Inteligencia y Seguridad de 2002 (o del espíritu de la misma) si de manera sistemática o consciente recibían datos de agencias de inteligencia extranjeras sobre residentes holandeses, mientras que no podían haber recopilado estos datos en virtud de sus propios poderes. En estos casos, las restricciones impuestas a los servicios de inteligencia por la Ley de 2002 podían convertirse en letra muerta. Sin embargo, los demandantes no justificaron u ofrecieron pruebas de que los servicios de inteligencia holandeses aprovecharan sistemática o conscientemente tal discrepancia entre el derecho holandés y los derechos extranjeros.

260. El recurso de casación, basado principalmente en supuestos errores en la interpretación de las demandas de los demandantes por el Tribunal de Apelación y en el alcance de la carga de la prueba que se les impuso, fue desestimado por el "Hoge Raad" (Tribunal Supremo) el 7 de septiembre de 2018 (ECLI:NL:HR:2018:1434).

D. Estados Unidos de América.

261. Los servicios de inteligencia de los Estados Unidos utilizan el programa Upstream de conformidad con la sección 702 de la FISA.

262. El Fiscal General y el Director Nacional de Inteligencia emiten certificaciones anuales que autorizan la vigilancia dirigida a personas no estadounidenses que se cree razonablemente que se encuentran fuera de los Estados Unidos de América. No tienen que especificar al FISC las personas no nacionales de los EEUU en particular que son su objetivo, y no hay ningún requisito que exija demostrar que existen motivos para creer que un individuo objetivo es un agente de una potencia extranjera. En su lugar, las certificaciones de la sección 702 identifican las categorías de información que pueden ser recopiladas, las cuales han de cumplir con la definición legal de información de inteligencia extranjera. Las certificaciones autorizadas incluían información sobre terrorismo internacional y la adquisición de armas de destrucción masiva.

263. De conformidad con la autorización, la NSA, con la obligada asistencia de los proveedores de servicios, copia y realiza búsquedas de flujos del tráfico de Internet a medida que los datos fluyen a través de Internet. Tanto las llamadas telefónicas como las comunicaciones por Internet son recopiladas. Antes de abril de 2017, la NSA adquirió transacciones de Internet que eran "para", "desde" o "acerca de" un selector específico. Una comunicación "a" o "desde" era una comunicación en la cual el remitente o un destinatario era un usuario de un selector específico de la sección 702. Una comunicación "acerca de" era aquélla en la que se hacía referencia al selector específico dentro de la transacción de Internet adquirida, pero el objetivo no era necesariamente un participante en la comunicación. Las comunicaciones "sobre" implicaban, por tanto, buscar en el contenido de las comunicaciones que atravesaban Internet. Sin embargo, desde abril de 2017 en adelante, la NSA no ha adquirido o

recopilado comunicaciones que son simplemente "sobre" un objetivo. Además, la NSA declaró que, como parte de esta reducción, eliminaría la gran mayoría de las comunicaciones de Internet previamente adquiridas mediante Upstream tan pronto como fuera posible.

264. La sección 702 exige que el Gobierno desarrolle procedimientos de fijación de objetivos y de minimización los cuales se mantengan bajo la revisión del FISC.

265. La Orden Ejecutiva 12333, suscrita en 1981, autoriza la recopilación, retención y difusión de la información obtenida en el curso de actividades legales de inteligencia extranjera, contrainteligencia, investigaciones internacionales de narcóticos o de terrorismo internacional. La vigilancia de extranjeros bajo la Orden Ejecutiva 12333 no está sujeta a la regulación nacional de la FISA. No se sabe cuántos datos se recopilan bajo la Orden Ejecutiva 12333, en relación con las obtenidos bajo la sección 702.

LA LEY

266. Coincidentemente, los demandantes en los tres casos acumulados alegaron la incompatibilidad con los artículos 8 y 10 de tres regímenes diferenciados: el régimen de interceptación masiva de comunicaciones en virtud de la sección 8 (4) de la Ley de Regulación de Poderes de Investigación de 2000 ("RIPA"); el régimen para la recepción de inteligencia de servicios de inteligencia extranjeros; y el régimen de adquisición de datos de comunicaciones a partir de proveedores de servicios comunicaciones ("CSPs").

267. Antes de tratar cada uno de estos regímenes de forma individualizada, la Gran Sala abordará una cuestión preliminar.

I. CUESTIÓN PRELIMINAR ANTE LA GRAN SALA

268. Según reiterada jurisprudencia del Tribunal, el "caso" remitido a la Gran Sala abarca necesariamente todos los aspectos de la demanda previamente examinados por la Sala en su Sentencia. El "caso" remitido a la Gran Sala abarca la demanda que ya ha sido declarada admisible, así como las reclamaciones que no han sido declaradas inadmisibles (ver *S.M. contra Croacia* [GC], núm. 60561/14, § 216, 25 de junio de 2020, y los documentos citados en el mismo).

269. Los demandantes en el presente caso presentaron sus reclamaciones en 2013, 2014 y 2015, respectivamente. Dichas reclamaciones se referían principalmente a las actividades de vigilancia bajo la RIPA y los Códigos de Práctica relacionados. Posteriormente se modificaron los Códigos de prácticas. Más significativamente, la Ley de Poderes de Investigación de 2016 ("IPA") recibió la sanción real el 29 de noviembre de 2016 y sus disposiciones comenzaron a entrar en vigor a partir del diciembre de 2016 en adelante. Los nuevos regímenes de vigilancia establecidos en la IPA eran operativos en su mayoría desde el verano de 2018. Las disposiciones del Capítulo I de la Parte I de la RIPA fueron derogadas a lo largo de 2018.

270. La Sala examinó el cumplimiento del Convenio por la ley vigente en la fecha en que se examinó la admisibilidad de las demandas de los demandantes; es decir, consideró la ley tal como estaba vigente el 7 de noviembre de 2017. Por ser ésta la "demanda que había sido declarada admisible", la Gran Sala debe, asimismo, limitar su examen al régimen legislativo tal como se establece el 7 de noviembre de 2017. Esto es lo oportuno, ya que los regímenes legales que se introdujeron gradualmente tras la

entrada en vigor de la IPA están actualmente sujetos a impugnación ante los tribunales nacionales y no estaría abierta a la Gran Sala la posibilidad de examinar la nueva legislación antes de que esos tribunales hayan tenido oportunidad de hacerlo.

271. Los demandantes no han impugnado la conclusión de la Sala de que el Tribunal de Poderes de Investigación ("IPT") es ahora un recurso eficaz tanto para las reclamaciones individuales como para las reclamaciones generales relativas al cumplimiento del Convenio por el régimen de vigilancia, y el Gobierno no impugnó su conclusión de que, en las circunstancias del caso, los demandantes habían agotado los recursos internos en el sentido del artículo 35.1 del Convenio. Por tanto, ninguna de las dos cuestiones deben ser evaluadas por la Gran Sala.

II. LA INTERCEPCIÓN MASIVA DE LAS COMUNICACIONES

A. Jurisdicción territorial

272. Con respecto al régimen de la sección 8, (4), el Gobierno no planteó objeción en virtud del artículo 1 del Convenio, ni sugirió que la interceptación de comunicaciones se estaba llevando a cabo fuera de la jurisdicción territorial del Estado. Además, durante la vista ante la Gran Sala el Gobierno confirmó expresamente que no habían planteado objeción por este motivo, ya que al menos algunos de los demandantes estaban claramente dentro de la jurisdicción territorial del Estado. Por lo tanto, a los efectos del presente caso, el Tribunal procederá asumiendo que, en la medida en que los demandantes realizan una reclamación acerca del régimen del artículo 8 (4), los asuntos sobre los que reclaman entran dentro de la competencia jurisdiccional del Reino Unido.

B. La violación del artículo 8 del Convenio alegada.

273. Los demandantes de los tres casos acumulados plantearon que el régimen de interceptación masiva de comunicaciones era incompatible con el artículo 8 del Convenio, que establece que:

> "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
>
> 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."

1. La sentencia de la Sala.

274. La Sala reconoció expresamente que los Estados disfrutaban de un amplio margen de apreciación para decidir qué tipo de régimen de interceptación era necesario para proteger la seguridad nacional, pero consideró que la discrecionalidad otorgada a los Estados en el funcionamiento de un régimen de interceptación debía ser necesariamente más limitada. Al respecto, observó que el Tribunal había identificado seis "salvaguardas mínimas" que debían preverse en la ley para evitar abusos de poder: la naturaleza de los delitos que pueden dar lugar a una orden de interceptación, una definición de las categorías de personas susceptibles de que sus comunicaciones fueran interceptadas, un límite en la duración de la interceptación, el procedimiento a seguir para examinar, utilizar y almacenar los datos obtenidos, las precauciones que deberían tomarse al

comunicar los datos a terceros, y las circunstancias en las que los datos interceptados podían o debían ser eliminados o destruidos. Estas salvaguardas, que se establecieron por primera vez en *Huvig c. Francia*, 24 de abril de 1990, § 34, Serie A núm. 176 B y *Kruslin c. Francia*, 24 de abril 1990, § 35, Serie A núm. 176-A, habían sido aplicadas rutinariamente por el Tribunal en su jurisprudencia sobre la interceptación de comunicaciones y en dos casos específicamente en lo que respecta a la interceptación masiva de comunicaciones (ver *Weber y Saravia c. Alemania* (dec.), núm. 54934/00, TEDH 2006 - XI y *Liberty y otros contra el Reino Unido*, núm. 58243/00, 1 de julio de 2008).

275. En opinión de la Sala, la decisión de utilizar un régimen de interceptación masiva estaba dentro del margen de apreciación otorgado a los Estados Contratantes. Evaluó el funcionamiento del régimen de interceptación masiva del Reino Unido por referencia a las seis salvaguardas mínimas establecidas en el párrafo anterior. Como las dos primeras salvaguardas no se aplicaban fácilmente a la interceptación masiva, la Sala reformuló estas salvaguardas, considerando primero, si los motivos por los que se podía emitir una orden de interceptación eran suficientemente claros; en segundo lugar, si la legislación nacional proporcionaba a los ciudadanos una indicación adecuada de las circunstancias en las que sus comunicaciones podían ser interceptadas; y en tercer lugar, si el derecho interno brindaba a los ciudadanos una indicación adecuada de las circunstancias en las que sus comunicaciones podían ser seleccionadas para examen. Además, a la luz de la jurisprudencia reciente (incluida *Roman Zakharov contra Rusia* [GC], núm. 47143/06, TEDH 2015) la Sala también tuvo en cuenta las disposiciones para supervisar la implementación de medidas de vigilancia secreta, la existencia de mecanismos de notificación y cualquier recurso previsto por la legislación nacional.

276. Identificó las siguientes dos áreas de preocupación respecto al régimen de la sección 8 (4): primero, la falta de supervisión de la selección de portadores para la interceptación, los selectores utilizados para filtrar las comunicaciones interceptadas, y el proceso por el cual los analistas seleccionaron las comunicaciones interceptadas para su examen; y, en segundo lugar, la ausencia de salvaguardas reales aplicables a la búsqueda y selección para el examen de los datos relacionados con las comunicaciones. En vista de la supervisión independiente proporcionada por el Comisionado de Intercepción de Comunicaciones (“el Comisionado IC”) y el IPT, y las extensas investigaciones independientes que siguieron a las revelaciones de Edward Snowden, la Sala consideró que el Reino Unido no estaba abusando de sus poderes de interceptación masiva. Sin embargo, en vista de las deficiencias antes mencionadas, sostuvo, por mayoría, que la mayor parte del régimen de interceptación no cumplió con el requisito de “calidad de la ley” y era incapaz de mantener la “interferencia” a aquello que fuera “necesario en una sociedad democrática”.

2. Alegaciones de las partes

(a) Los demandantes.

277. Los demandantes alegaron que la interceptación masiva no era, en principio, ni necesaria ni proporcionada en el sentido del artículo 8 del Convenio y, como tal, no estaba dentro del margen de apreciación de los Estados. El asunto *Szabó y Vissy contra Hungría*, núm. 37138/14, 12 de enero de 2016 sugirió que una medida de vigilancia secreta tenía que ser “estrictamente necesaria” para salvaguardar las instituciones

democráticas y obtener inteligencia vital, y no se ha demostrado que la interceptación masiva satisfaga este requisito. Pese a que sin duda era de utilidad, se desprende de la jurisprudencia del Tribunal que no todo lo que fuera útil para los servicios de inteligencia era permisible en una sociedad democrática (ver *S. y Marper c. Reino* [GC], núms. 30562/04 y 30566/04, TEDH 2008).

278. Según los demandantes, las distintas interferencias sobre el derecho al respeto de la vida privada y la correspondencia del artículo 8 se produjeron con la interceptación de las comunicaciones (contenido y / o datos de comunicaciones); su almacenamiento; su procesamiento automatizado; y su examen. Mientras que coincidían en que se produjo una interferencia "sustancial" cuando eran examinadas las comunicaciones interceptadas, creyeron que era incorrecto sugerir que no se produjo ninguna interferencia "significativa" antes de este momento. Por el contrario, la jurisprudencia del Tribunal indicó que incluso el almacenamiento de información personal por parte del Estado equivalía a una grave injerencia en los derechos de una persona en virtud del artículo 8 del Convenio (véase, por ejemplo, *Rotaru c. Rumania* [GC], núm. 28341/95, TEDH 2000 *V y S. y Marper*, antes citada). Esto era especialmente así cuando los datos eran objeto de un tratamiento automatizado. De hecho, a medida que la potencia del procesamiento y el aprendizaje sobre las máquinas avanzaban rápidamente, el almacenamiento y el procesamiento electrónico de datos podían ser por sí mismos muy intrusivos, sin necesidad de que el contenido subyacente o los datos relacionados con las comunicaciones estuviesen siendo vistos por un individuo. Al respecto, los demandantes sostuvieron que, contrariamente a la "sopa amorfa" en la que confía el Gobierno (ver párrafo 288 siguiente), los datos recopilados se parecían más a "una biblioteca bien organizada e indexada en la que se puede encontrar rápidamente cualquier cosa que se desee". La disponibilidad del procesamiento automático planteó problemas de privacidad y no minimizó, como sostenía el Gobierno, ninguna intrusión.

279. Pese a que la Gran Sala considera que el uso de un régimen de interceptación masiva estaba dentro del margen de apreciación del Estado, los demandantes argumentaron que el régimen de la sección 8 (4) no era conforme con la Ley. En primer lugar, la RIPA era innecesariamente compleja, un hecho reconocido por todos los revisores independientes; tanto es así, de hecho, que la verdadera naturaleza y el alcance de la vigilancia que se estaba llevando a cabo solo se había aclarado gracias a las revelaciones de Edward Snowden. Además, las "disposiciones por debajo de la línea de flotación" habían sido establecidas por la propia GCHQ; ninguna fue accesible ni aprobada por el Parlamento; eran, como una cuestión de política interna, sujeta a cambios a voluntad del ejecutivo; y no eran vinculantes. Los demandantes, por lo tanto, argumentaron que no deberían tenerse en cuenta en el proceso análisis del Tribunal.

280. Al evaluar la previsibilidad, los demandantes argumentaron que los cambios tanto en la sociedad como en la tecnología determinaban la necesidad de que el Tribunal actualizara su enfoque actual, y mejorara las salvaguardas necesarias, para garantizar que los derechos del Convenio siguieran siendo prácticos y efectivos. La jurisprudencia del Tribunal existente sobre la interceptación masiva derivada de la decisión en el asunto *Weber y Saravia* (citada anteriormente), se remontaba a 2006, cuando el mundo era un lugar diferente. Los teléfonos inteligentes eran básicos y tenían funcionalidades limitadas; Facebook era utilizado principalmente por estudiantes universitarios; y Twitter estaba en su infancia. Hoy en día, las personas viven la mayor parte de sus vidas en línea, utilizando Internet para comunicarse, comunicar ideas, realizar

investigaciones, mantener relaciones, buscar consejo médico, llevar diarios, organizar viajes, escuchar música, orientarse y realizar transacciones financieras. Además, la tecnología moderna genera una enorme cantidad de datos de comunicaciones, que son muy reveladores incluso si no se examina el contenido, y que están estructurados de tal manera que los ordenadores pueden procesarlos y buscar patrones en ellos más rápido y con más eficacia que las búsquedas similares sobre el contenido. Por ejemplo, los teléfonos móviles generan constantemente datos de comunicaciones cuando se comunican con la red móvil, produciendo un registro de la ubicación del teléfono, lo que permite rastrear los movimientos del usuario y revelar su uso de Internet.

281. En opinión de los demandantes, las salvaguardas actualizadas y mejoradas deben incluir la previa autorización judicial independiente de las órdenes, de la elección de selectores y de la selección del material interceptado para su examen. Además, cuando los selectores o los términos de búsqueda hagan referencia a un individuo, deberían contar con una evidencia objetiva de sospecha razonable en relación con esa persona. Finalmente, también debe haber una notificación posterior de cualquier objetivo de vigilancia claramente definido, cuando no cause daño sustancial al interés público.

282. Los demandantes identificaron una serie de elementos del régimen de interceptación masiva del Reino Unido que consideraban inadecuados. En primer lugar, había una ausencia de independencia, y mucho menos judicial, respecto a la autorización de vigilancia. Si bien la autorización judicial podía no ser en sí misma una salvaguarda suficiente contra el abuso, esto no significaba que no fuera necesaria. Además, los demandantes consideraban que también debería haber una aprobación independiente, si no judicial, de los selectores y términos de búsqueda utilizados por la GCHQ. Sin embargo, ni los portadores que iban a ser interceptados ni los selectores fuertes se enumeraban en la orden.

283. En segundo lugar, la distinción entre comunicaciones internas y externas no sólo estaba mal definida, sino que también carecía de sentido, pues la mayoría de las comunicaciones era probable que se incluyeran en la categoría de “externas”. En opinión de los demandantes, era posible proporcionar una protección más significativa a las comunicaciones internas. Por ejemplo, en Suecia todas las comunicaciones internas tenían que ser destruidas inmediatamente si eran descubiertas.

284. En tercer lugar, existían salvaguardas limitadas respecto al contenido de las comunicaciones de personas que se conocía que se encontraban en las Islas Británicas, y no hubo salvaguardas en relación con sus datos de comunicaciones. La GCHQ pudo conservar la totalidad de los datos de comunicaciones obtenidos bajo el régimen de interceptación masiva, con sujeción únicamente a los límites en su capacidad de almacenamiento y el período máximo de conservación. Estos datos -que eran extremadamente intrusivos - podían ser buscados de acuerdo con un factor referido a una persona que se conociera que se encontraba en las Islas Británicas, sin ningún requisito relativo a que el Secretario de Estado primero certificara que la búsqueda era necesaria y proporcionada.

285. En cuarto lugar, el régimen no especificó, ni en la ley ni en detalle, el fin para el cual el material podía ser examinado y, de acuerdo con el Comité de Inteligencia y Seguridad del Parlamento (“el ISC”-siglas en inglés-), la descripción del material en el certificado de la Secretaría de Estado era “genérica”.

286. Por último, los demandantes alegaron que el Comisionado IC únicamente proporcionó supervisión a tiempo parcial y, con recursos limitados, siendo insuficiente para garantizar una supervisión sólida y significativa. La efectividad del IPT estaba igualmente limitada, ya que no podía proporcionar un remedio para la ausencia de autorización judicial previa y, en todo caso, las personas debían tener alguna base para creer que habían estado sujetos a vigilancia secreta antes de que el IPT aceptara sus reclamaciones.

(b) El Gobierno

287. El Gobierno alegó que la información obtenida en virtud del régimen de interceptación masiva fue fundamental para la protección del Reino Unido de las amenazas a la seguridad nacional. No solo les permitió descubrir amenazas hasta ahora desconocidas, sino que también les permitió llevar a cabo la vigilancia de objetivos conocidos fuera de su jurisdicción territorial. La imprevisibilidad de la ruta por la cual las comunicaciones electrónicas eran transmitidas (y el hecho de que esas comunicaciones se dividieran en paquetes que podían transmitirse a través de diferentes rutas) significaba que, para obtener, aunque fuera una pequeña proporción de las comunicaciones de objetivos conocidos en el extranjero, era necesario interceptar todas las comunicaciones que fluían por los portadores seleccionados. El poder de interceptación masiva había sido objeto de examen detallado y continuo por una serie de órganos independientes en los últimos años y hubo unanimidad de opinión de que no había "ninguna alternativa" ... "o combinación de alternativas suficientes para sustituir el poder de la interceptación masiva". Según el Gobierno, los Estados deberían tener derecho a un amplio margen de apreciación al juzgar qué sistemas eran necesarios para proteger a la comunidad en general de tales amenazas, y al someter esos sistemas a escrutinio, el Tribunal debe cuidarse de no socavar la eficacia de un medio de obtener inteligencia que salva vidas y que no se puede recopilar de ninguna otra manera.

288. El Gobierno sostuvo que la interceptación de las comunicaciones bajo el régimen de interceptación masiva sólo provocaría una interferencia significativa en los derechos del artículo 8 de una persona si sus comunicaciones fueran seleccionadas para su examen (es decir, fueran incluidas en un índice de comunicaciones a partir del cual un analista podía potencialmente elegir su contenido para inspeccionarlo) o realmente examinadas por un analista. No podía considerarse que sus derechos hubieran sido infringidos más allá del mínimo grado posible si la copia de una comunicación era descartada casi en tiempo real o mantenida durante unos días como máximo en una "sopa amorfa" general de datos; es decir, podía buscarse mediante selectores y consultas, pero no era examinada ni utilizada. La abrumadora mayoría de las comunicaciones que fluían a través de cada cable interceptado no podían ser "seleccionadas para examen", y por lo tanto tenían que ser descartadas.

289. En cuanto a las garantías necesarias, el Gobierno coincidió con la Sala en que era apropiado evaluar el régimen de interceptación masiva por referencia a los mismos estándares que habían sido desarrollados por el Tribunal en casos relacionados con la interceptación selectiva de comunicaciones. El Gobierno también estuvo de acuerdo en gran medida con la Sala respecto a la evaluación del régimen de la sección 8(4) por referencia a esos estándares. Reiteraron que no había posibilidad de que un analista viera ninguna comunicación a menos que y hasta que hubieran sido seleccionada para su examen después de un proceso de cribado automatizado; la selección y cualquier

examen subsiguiente eran controlados muy cuidadosamente; no se podía hacer ningún informe de inteligencia sobre ninguna comunicación o datos de comunicaciones a menos que hubieran sido vistos por un analista; la sección 16 (2) de la RIPA requería que el Secretario de Estado certificara la necesidad y proporcionalidad de la búsqueda del contenido de las comunicaciones de acuerdo con un factor atribuible a un individuo que se conocía que se encontraba en las Islas Británicas; y las funciones de supervisión combinadas del ISC, el Comisionado IC y el IPT cumplieron con los requisitos del Convenio. En todas las etapas del proceso de interceptación masiva, las salvaguardas aplicables fueron construidas en torno a los conceptos de necesidad y proporcionalidad del Convenio. Esos principios fundamentales regían en primer lugar la obtención del material, su examen, manejo, almacenamiento, divulgación, conservación y eliminación.

290. Respecto a aquellos aspectos del régimen que, según la Sala, no habían proporcionado las salvaguardas adecuadas contra los abusos, el Gobierno proporcionó más aclaraciones. Primero que nada, aunque reconocieron que la orden no especificaba los portadores individuales que serían objeto de interceptación, ya que habría graves problemas de impracticabilidad y dificultades para incluir esta información en la orden, no obstante, contenía una descripción de lo que iba a implicar la interceptación y una descripción de los tipos de portadores que serían interceptados. La GCHQ informó regularmente al Comisionado IC sobre la base sobre la cual se seleccionaban los portadores para la interceptación.

291. En segundo lugar, aclararon que la elección de los selectores era en la práctica cuidadosamente controlada. Siempre que se agregaba un nuevo selector al sistema, el analista tenía que completar un registro escrito, explicando por qué era necesario y proporcionado aplicar el selector para los fines previstos en el certificado del Secretario de Estado. Esto se hizo mediante la selección del texto de un menú desplegable, seguido de la adición, por parte del analista, de un texto libre explicando por qué era necesario y proporcionado realizar la búsqueda. En el caso de un "selector fuerte", el analista tenía que explicar, por ejemplo, la justificación para buscar las comunicaciones de un objetivo en particular; cómo el selector estaba relacionado con el método de comunicación del objetivo; y por qué la selección de las comunicaciones pertinentes no implicaba un grado inaceptable de intrusión colateral en la privacidad. En el caso de una nueva "consulta compleja", el analista tenía que desarrollar los criterios de selección más probables para identificar comunicaciones de valor para la inteligencia, y tenía que explicar por qué los criterios estaban justificados y por qué su uso era necesario y proporcionado para los fines previstos en el certificado del Secretario de Estado. Los selectores utilizados para el desarrollo de objetivos o el descubrimiento de objetivos podían permanecer en uso durante un máximo de tres meses antes de que fuera necesaria su revisión.

292. Cualquier selector tenía que ser lo más específico posible para seleccionar el material mínimo necesario para el fin de inteligencia, y ser proporcionado. Si, a través del análisis, se establecía que los selectores no estaban siendo utilizados para el objetivo previsto, se tenía que tomar la acción inmediata de eliminarlos del sistema. El uso de selectores tenía que ser registrado en una ubicación aprobada que les permitiera ser auditados; creando un buscador de selectores en uso; y permitiendo la supervisión por parte del Comisionado IC. Por lo tanto, dentro de los poderes del Comisionado IC se encontraba una supervisión sólida e independiente de los selectores y los criterios de

búsqueda: en el momento en el que redactó su informe de 2014, se habían establecido específicamente sistemas y procesos para asegurar que realmente esto ocurría y, tras la sentencia de la Sala, el Gobierno había trabajado con la Oficina del Comisionado IC para garantizar que hubiera una supervisión mejorada de los selectores y criterios de búsqueda bajo la IPA. Sin embargo, el Gobierno afirmó que la autorización judicial previa no habría sido posible para cada selector sin alterar sustancialmente su capacidad para descubrir y repeler amenazas. Los sistemas de la GCHQ necesariamente trabajaban con muchos miles de selectores que a veces tenían que cambiar rápidamente para seguir el ritmo de las investigaciones y los descubrimientos de amenazas que avanzan rápidamente.

293. Las comunicaciones a las que solo se les aplicaba un "selector fuerte" eran descartadas inmediatamente a menos que coincidieran con el selector fuerte. Las comunicaciones a las que también se les aplicaba una "consulta compleja" eran retenidas por unos días, con el fin de permitir la realización del proceso, y luego se eliminaban automáticamente, a menos que se hubieran seleccionado para examen. Las comunicaciones que habían sido seleccionadas para su examen sólo podían conservarse cuando era necesario y proporcionado hacerlo. La posición predeterminada era que el período de retención de las comunicaciones seleccionadas no fuera más de unos pocos meses, después de los cuales eran eliminadas automáticamente (aunque si el material había sido citado en informes inteligencia, el informe se mantenía). En circunstancias excepcionales, podían retenerse las comunicaciones seleccionadas por más tiempo, según lo previsto en el Código de prácticas de interceptación de comunicaciones ("el Código IC").

294. El Gobierno reiteró que los analistas que examinaron el material seleccionado tenían que estar especialmente autorizados para hacerlo y recibían formación periódica obligatoria, incluida formación sobre los requisitos de necesidad y proporcionalidad. También eran evaluados. Antes de que examinaran el material, tenían que crear un registro que estableciera por qué el acceso al material requerido era coherente con el certificado del Secretario de Estado y los requisitos de la RIPA; y por qué era proporcionado (incluyendo las consideraciones relativas a cualquier circunstancia que pudiera dar lugar a un grado de violación colateral de la privacidad). A menos que tal registro hubiera sido creado, los sistemas de la GCHQ no permitían el acceso al material.

295. En cuanto a las salvaguardas relativas a los datos de comunicaciones, el Gobierno argumentó que examinar el contenido de los temas más sensibles y las comunicaciones privadas siempre implicaba un mayor grado de intrusión que examinar los datos de comunicaciones, independientemente de si esos datos eran agregados para proporcionar una imagen detallada de dónde se encontraba un individuo ubicado, qué sitios web visitó o con quién eligió comunicarse. Sobre esa base, seguía siendo apropiado que las normas que rigen contenido fueran más exigentes que las que rigen los datos de comunicaciones. Sin embargo, el Gobierno aceptó que el Secretario de Estado debía ser requerido para certificar la necesidad de examinar los datos de comunicaciones bajo una orden de interceptación masiva de conformidad con un régimen análogo (aunque no idéntico) al régimen de certificación vigente para el contenido de comunicaciones bajo la sección 16 de la RIPA. El nuevo Código de prácticas iba a ser modificado a tales efectos.

296. Hasta entonces, sin embargo, los datos relacionados con las comunicaciones estaban sujetos al mismo proceso de filtrado inicial que el contenido, mediante el cual los sistemas de procesamiento de la GCHQ descartaban automáticamente ciertos tipos de comunicaciones casi en tiempo real. Luego eran sometidos por medios automatizados a consultas simples o complejas. Sin embargo, había dos diferencias principales entre el tratamiento del contenido y el tratamiento de los datos relacionados con las comunicaciones. En primer lugar, las salvaguardas previstas en la sección 16 - que disponía que, para ser examinado, el material tenía que estar previsto en el certificado del Secretario de Estado y no podía seleccionarse de acuerdo con un factor referido a un individuo que se conocía que se encontraba en las Islas Británicas y cuyo fin era identificar sus comunicaciones – solo se aplicaba al contenido. De acuerdo con el Gobierno, no sería factible aplicar esta salvaguarda a datos relacionados con las comunicaciones. Se realizaron muchas más consultas de datos de comunicaciones (hasta varios miles en una semana) y en un gran número de casos la identidad de la persona a quien podían relacionarse los datos era desconocida. Además, los datos de comunicaciones a menudo tenían una utilidad temporal, y tener que retrasar la realización de búsquedas de dichos datos en espera de la adquisición de una autorización individual implicaba un grave riesgo de socavar su utilidad en términos de inteligencia. Requerir que el Secretario de Estado certificara la necesidad y proporcionalidad en cada caso individual, antes de que se llevaran a cabo las búsquedas, no era posible.

297. En segundo lugar, los datos relacionados con las comunicaciones que no eran seleccionados para examen no eran eliminados inmediatamente. La razón principal era que los datos de comunicaciones se utilizaban en gran medida para descubrir amenazas u objetivos de los que la GCHQ podía no haber tenido conocimiento anteriormente. Esto, por lo tanto, requería un mayor trabajo analítico, durante un período prolongado, para descubrir "incógnitas desconocidas". Ese descubrimiento muy a menudo podía implicar un ejercicio de unir pequeños elementos dispares de datos de comunicaciones para formar un "rompecabezas" que revelara una amenaza; e incluía la posibilidad de examen de elementos que inicialmente parecían no ser de interés de inteligencia. Descartar datos de comunicaciones no seleccionados inmediatamente, o después de unos pocos días, haría imposible este ejercicio.

298. No obstante, el Gobierno confirmó que antes de que cualquier analista pudiera examinar cualquier dato de comunicaciones, tenía que completar un registro explicando por qué era necesario y proporcionado hacerlo, en ejercicio de las funciones legales de la GCHQ. Por lo tanto, se generaba un registro auditable, exponiendo la justificación para el examen, y estos registros estaban disponibles para su inspección. Además, no se podían realizar informes de inteligencia sobre la base de datos de comunicaciones a menos y hasta que hubieran sido examinados. Por último, los datos relacionados con comunicaciones se podían conservar solo cuando fuera necesario y proporcionado hacerlo, por un período máximo de varios meses, a menos que se excepcionalmente se pudieran retener por más tiempo. De lo contrario los datos relacionados con las comunicaciones se eliminaban automáticamente una vez que el período máximo había expirado.

299. Finalmente, a la luz de la sentencia de la Sala el Gobierno confirmó que estaba tomando medidas para garantizar que cuando los datos sin contenido debían ser seleccionados para el examen por referencia a una persona que se creía que se

encontraba en las Islas Británicas, la selección tenía que ser certificada por el Secretario de Estado como necesaria y proporcionada sobre una base temática específica. Estando pendiente la introducción de un régimen "temático" de certificación, mediante cambios en el código que rige la interceptación de comunicaciones bajo la IPA, la GCHQ había estado trabajando con la oficina del Comisionado IC para generar información de gestión que pudiera ser utilizada por el Comisionado IC para mejorar la supervisión *ex post facto* de los datos relacionados con las comunicaciones. En particular, la GCHQ había realizado cambios en sus sistemas para que, en cualquier caso, cuando un analista pretendiera seleccionar datos secundarios para su examen en relación con una persona que se creía que se encontraba en las Islas Británicas por referencia a un factor relacionado a esa persona, esos casos se marcarían junto con la oportuna justificación para seleccionar los datos relevantes.

3. Alegaciones de terceros

(a) El Gobierno de Francia

300. El Gobierno francés alegó que ante amenazas tales como la delincuencia internacional y transfronteriza, y en vista de la creciente sofisticación de las tecnologías de la comunicación, la vigilancia masiva estratégica de las comunicaciones era de vital importancia para los Estados para la protección de la sociedad democrática. Además, era un error suponer que la interceptación masiva suponía una mayor intrusión en la vida privada que la interceptación individual dirigida, la cual, debido a su naturaleza, era más probable que diera como resultado la adquisición y el examen de un gran volumen de comunicaciones. En su opinión, no había motivos para que los criterios establecidos por el Tribunal en el asunto *Weber y Saravia* (citada arriba) no pudieran ser considerados igualmente pertinentes para la supervisión efectiva de la interceptación de datos y su procesamiento bajo un régimen de interceptación masiva. Sin embargo, estos criterios debían aplicarse en el contexto de una evaluación general, sopesando cualquier insuficiencia frente a las garantías existentes y la eficacia de las salvaguardas contra el abuso.

301. No había justificación para añadir la necesidad de que existieran "sospechas razonables" a estos criterios. En general, las autoridades no estaban en posición de saber de antemano de quiénes podía ser útil para ellos monitorear las comunicaciones electrónicas en interés de la ley y el orden o la seguridad nacional, y tal requisito privaría a la medida de vigilancia de todo interés operativo. Además, en opinión del Gobierno, no era necesario que se involucrara a una autoridad judicial en la autorización de tales operaciones de inteligencia, o para realizar un control *ex post facto*, siempre que la autoridad que concediera la autorización fuera independiente del ejecutivo, la autoridad de control del organismo estuviera dotada de facultades y competencias suficientes para ejercer un control efectivo y continuo, y los dos cuerpos fueran independientes uno del otro.

302. Finalmente, el Gobierno interviniente alegó que los metadatos eran por su naturaleza menos intrusivos que el contenido, ya que claramente contenían menos información sensible sobre el comportamiento y la vida privada de la persona en cuestión. Esta opinión fue apoyada por el informe de la Comisión de Venecia (véanse los párrafos 196-201 anteriores) y el TJUE en el asunto *Derechos Digitales* (véanse los párrafos 209 a 213 anteriores).

(b) El Gobierno de los Países Bajos

303. El Gobierno de los Países Bajos también planteó que la interceptación masiva era necesaria para identificar amenazas a la seguridad nacional que hasta ahora eran desconocidas. Para proteger la seguridad nacional, los servicios de inteligencia necesitaban las herramientas para investigar las amenazas emergentes de manera oportuna y eficaz. Para ello precisaban de los poderes necesarios que les permitieran detectar y/o prevenir no solo las actividades terroristas (como la planificación de ataques, reclutamiento, propaganda y financiación), sino también poderes intrusivos frente a las actividades cibernéticas de los actores, estatales o no estatales, destinadas a perturbar la democracia (por ejemplo, mediante la influencia en las elecciones nacionales o la obstrucción de las investigaciones de las autoridades nacionales y organizaciones internacionales. Un ejemplo de esto fue el intento de hackeo de la investigación del uso de armas químicas en Siria por parte de la Organización para la Prohibición de las Armas Químicas en La Haya). Además, la creciente dependencia de sectores vitales de las infraestructuras de la tecnología digital significaba que dichos sectores, incluida la gestión del agua, energía, telecomunicaciones, transporte, logística, puertos y aeropuertos, eran cada vez más vulnerables a los ciberataques. Las consecuencias de la disrupción en tales sectores tendrían un profundo impacto en la sociedad, mucho más allá de los sustanciales daños económicos.

304. Un factor que complicaba todo esto era el desarrollo de nuevos medios de comunicación digital y el aumento exponencial de los datos que eran transmitidos y almacenados globalmente. En muchos casos, se desconocía la naturaleza y el origen de una amenaza particular y el uso de la interceptación dirigida no era factible. Sin embargo, aunque la interceptación masiva no estaba tan definida como la interceptación dirigida, nunca estuvo completamente desvinculada. Asimismo, se aplicaba con fines específicos.

305. En opinión del Gobierno interviniente, no eran necesarias salvaguardas mínimas adicionales o actualizadas; aquéllas previamente identificadas por el Tribunal eran suficientemente sólidas y “a prueba de futuro”. Los requisitos adicionales propuestos por los demandantes ante la Sala - en particular, el requisito de demostrar una “sospecha razonable” - reducían inaceptablemente la eficacia de los servicios de inteligencia sin proporcionar ninguna protección adicional significativa a los derechos fundamentales.

306. Además, según el Gobierno interviniente, era relevante distinguir entre el contenido y los datos relacionados con las comunicaciones, ya que era probable que el contenido de las comunicaciones fuera más sensible que los datos relacionados con las comunicaciones. El Gobierno interviniente también estuvo de acuerdo con la Sala en que no era correcto asumir automáticamente que la interceptación masiva constituía una mayor intrusión en la vida privada de un individuo que la interceptación dirigida, ya que con la intercepción dirigida era probable que todas, o casi todas, las comunicaciones interceptadas fueran analizadas. Esto no era así en el caso de la interceptación masiva, donde las restricciones en el examen y el uso de datos determinaban la intrusión de la interceptación en los derechos fundamentales de las personas.

307. Finalmente, el Gobierno interviniente alegó que cualquier requisito de explicar o fundamentar los selectores o los criterios de búsqueda en la autorización restringiría seriamente la efectividad de la interceptación masiva en vista del alto grado de

incertidumbre sobre el origen de una amenaza. La supervisión *ex post* proporcionaba garantías suficientes.

(c) El Gobierno de Noruega

308. El Gobierno de Noruega sostuvo que, con respecto a la decisión de los Estados de introducir y operar a través de algún régimen de interceptación masiva por motivos de seguridad nacional, el margen de apreciación tenía que ser amplio. Esto se debía a que los servicios de inteligencia tenían que seguir el ritmo de los rápidos avances en la tecnología de la información y las comunicaciones. Los actores hostiles cambiaban sus dispositivos e identidades digitales a un ritmo que dificultaba la labor de rastrearlos a lo largo del tiempo. También era difícil descubrir y contrarrestar operaciones cibernéticas hostiles de manera oportuna sin herramientas capaces de descubrir anomalías y firmas relevantes. Por lo tanto, no había duda de que se necesitaba de facultades modernas como la intercepción masiva para encontrar las amenazas desconocidas que operan en el dominio digital, y permitir a los servicios descubrir y seguir las amenazas de inteligencia relevantes.

309. En opinión del Gobierno de Noruega, la supervisión del Tribunal debía basarse en una evaluación general de si las salvaguardas del procedimiento contra los abusos eran adecuadas y suficientes. Debían evitarse los requisitos absolutos. Tampoco debían aplicarse criterios que socavaran indirectamente el amplio margen de apreciación concedido a los Estados para decidir sobre la utilización de un régimen de interceptación masiva por razones de seguridad nacional. El requisito de "sospecha razonable" o "notificación posterior" tendría este efecto.

310. Finalmente, el Gobierno interviniente alentó al Tribunal a abstenerse de importar conceptos y criterios del TJUE. En primer lugar, en el momento temporal que se estaba enjuiciando, diecinueve Estados contratantes del Consejo de Europa no eran miembros de la Unión Europea. En segundo lugar, mientras que el Convenio y la Carta de los Derechos Fundamentales tenía muchas características en común, había también diferencias, en particular el artículo 8 de la Carta contenía un derecho a la protección de datos personales. El TJUE también formuló el concepto de "proporcionalidad" de manera diferente, usando un método de "estricta necesidad" que no era comparable con el utilizado por el Tribunal.

(d) El Relator Especial de las Naciones Unidas sobre la promoción del derecho a la libertad de opinión y expresión.

311. El Relator Especial argumentó que la vigilancia ensombrecía las comunicaciones, de modo que las personas podían abstenerse de participar en actividades protegidas por el derecho internacional sobre los derechos humanos. Eso no quería decir que todos los operativos de vigilancia constituyeran una violación de las leyes de derechos humanos; algunos podían ser tolerables cuando las condiciones de legalidad, necesidad y legitimidad se cumplían. Sin embargo, todos los tipos de vigilancia requerían una rigurosa evaluación de si eran acordes con las normas de derecho internacional sobre los derechos humanos.

312. En opinión del Relator Especial, el derecho a la intimidad debía ser protegido no solo como un derecho fundamental independiente de todos los demás, sino también con el fin de proteger otros derechos, como la libertad de opinión y expresión, que

dependían de una zona de privacidad para su disfrute. Como el Relator Especial había indicado en su informe de 2015 los sistemas de vigilancia podían socavar el derecho a formarse una opinión y el miedo a la divulgación involuntaria de la actividad en línea podía disuadir a las personas de acceder a la información.

313. El informe del Alto Comisionado de la ONU desaconsejaba distinguir los metadatos del contenido al examinar la gravedad de la injerencia en los derechos protegidos por el Pacto Internacional de Derechos Civiles y Derechos Políticos ("PIDCP"). Su informe de 2014 indicó que la obtención de metadatos por medio de la vigilancia gubernamental podía revelar detalles más privados sobre un individuo que incluso quizás una comunicación privada. El Relator Especial indicó además que la distinción entre comunicaciones internas y externas podía ser contraria al Pacto Internacional de Derechos Civiles y Políticos. El Pacto Internacional de Derechos Civiles y Políticos colocó a los Estados bajo el deber de respetar y garantizar todos los derechos previstos en el mismo para todas las personas dentro de su jurisdicción, y en su última Observación General el Comité de Derechos Humanos interpretó este estándar en el sentido de que incluía las actividades estatales que impactaran directamente en derechos fuera de sus territorios.

314. Por último, el Relator Especial destacó la importancia de las salvaguardas para proporcionar protección contra los abusos, en particular, la necesidad de que un juzgado, tribunal u otro órgano jurisdiccional supervisara la aplicación de una medida de interferencia; la notificación posterior a los sujetos de la vigilancia; la publicación de información sobre el alcance de las técnicas de vigilancia y poderes; y el derecho a un recurso efectivo en caso de abuso.

(e) Access Now

315. Access Now alegó que la vigilancia masiva en el presente caso no cumplió con el Pacto Internacional de Derechos Civiles y Políticos y los Principios Internacionales de Derechos Humanos aplicables a la vigilancia de las comunicaciones puesto que el Reino Unido no había demostrado que tal vigilancia fuera estrictamente necesaria o proporcionada. Además, sostuvo que los programas de vigilancia no debían considerarse de forma independiente, sino que debían considerarse en relación con la totalidad de actividades de vigilancia de una nación como el aprendizaje automático, a través del cual mediante algoritmos matemáticos podían producirse inferencias en colecciones de datos, que había aumentado la invasividad en grandes conjuntos de datos y minería de datos.

(f) Artículo 19

316. Artículo 19 sostuvo lo indiscriminado y sin sospechas de la recopilación, y que el análisis y la conservación de las comunicaciones de las personas eran inherentemente desproporcionadas. En opinión de Artículo 19, solo la vigilancia dirigida basada en sospechas razonables y autorizada por un juez constituía una restricción legítima a los derechos de privacidad.

(g) European Digital Rights ("EDRi") y otras organizaciones activas en el ámbito de los derechos humanos en la sociedad de la información.

317. La EDRi y otros argumentaron que el presente caso ofrecía al Tribunal una oportunidad crucial para revisar su posición sobre la protección de los metadatos. Los

gobiernos habían construido sus programas de vigilancia basándose en la distinción establecida entre contenido y metadatos en el asunto *Malone c. Reino Unido*, de 2 de agosto de 1984, Serie A núm. 82, pero en el momento en el que ese caso fue enjuiciado ni Internet ni los teléfonos móviles existían. Hoy, los metadatos podían pintar una imagen detallada e íntima de una persona: permitían el mapeo de sus redes sociales, el seguimiento de su ubicación, el seguimiento de su navegación por Internet, el mapeo de sus patrones de comunicación y el conocimiento de quién es una persona con la que ha interactuado. Además, el nivel de detalle que se podía obtener aumentaba cuando se analizaba a gran escala. De hecho, Stewart Baker, abogado general de la NSA, había indicado que los metadatos podían revelar todo sobre la vida de alguien, y que, si se tuvieran suficientes metadatos, no se precisaría del contenido. En consecuencia, no debían ser concedidos diferentes grados de protección a los datos personales sobre la base de la distinción arbitraria e irrelevante entre contenido y metadatos, sino también sobre la base de las inferencias que podían derivarse de los datos.

(h) Iniciativa de Justicia de la Sociedad Abierta ("OSJI")

318. La OSJI sostuvo que tanto la cantidad de datos disponibles para interceptación hoy en día como el apetito de los gobiernos por los datos superaban con creces lo que era posible en el pasado. En consecuencia, la interceptación masiva era una interferencia grave en la privacidad que podía, a través de su "efecto paralizador", interferir potencialmente con otros derechos como la libertad de expresión y la libertad de asociación. Por lo tanto, para que fuera legal, la interceptación masiva debía satisfacer varias condiciones previas: la ley aplicable tenía que ser suficientemente precisa; el alcance de la información recopilada tenía que estar limitado en el tiempo y en el espacio; y la información solo debía recopilarse sobre la base de una "sospecha razonable".

(i) La Fundación de Helsinki para los Derechos Humanos ("HFHR")

319. La HFHR describió su experiencia desafiando la vigilancia de las comunicaciones de las autoridades públicas de Polonia, que culminó en el Tribunal Constitucional que consideró que ciertos aspectos de la legislación eran inconstitucionales. Posteriormente se modificó la legislación.

(j) La Comisión Internacional de Juristas ("CIJ")

320. La CIJ sostuvo que, a la luz de la escala y el alcance de la interferencia con la privacidad que implica la vigilancia masiva, la distinción entre los metadatos y el contenido se había vuelto obsoleta. Además, el hecho de que, en una operación de vigilancia masiva, la interferencia de derechos pudiera tener lugar fuera de la jurisdicción territorial de un Estado no excluía la responsabilidad de ese Estado, ya que su control sobre la información era suficiente para establecer su jurisdicción.

(k) La Sociedad de Abogados de Inglaterra y Gales.

321. La Sociedad de Abogados de Inglaterra y Gales expresó su profunda preocupación por las implicaciones del régimen de la sección 8(4) sobre el principio de secreto profesional. En su opinión, el régimen permitía la interceptación de comunicaciones legalmente privilegiadas y confidenciales entre abogados y clientes, aun cuando ambos se encontraran en el Reino Unido. También permitía la recolección rutinaria de los metadatos adjuntos a dichas comunicaciones. Además, una vez interceptadas estas

comunicaciones legalmente privilegiadas podían ser utilizadas, siempre que el fin principal y el objeto de la orden fuera la obtención de comunicaciones externas. Estas disposiciones, y la ausencia de limitaciones adecuadas en el uso de dicho material, era probable que tuvieran un impacto potencialmente grave y un efecto escalofriante en la franqueza y apertura de las comunicaciones abogado-cliente.

4. Evaluación del Tribunal

(a) Observaciones preliminares

322. La presente reclamación se refiere a la interceptación masiva de comunicaciones transfronterizas por parte de los servicios de inteligencia. Si bien no es la primera vez que el Tribunal ha valorado este tipo de vigilancia (ver los asuntos *Weber y Saravia* y *Liberty y Otros*, ambos anteriormente citadas), en el transcurso del procedimiento, se ha puesto de manifiesto que la evaluación de un régimen de este tipo plantea dificultades específicas. En la actualidad, cada vez más digital, la gran mayoría de las comunicaciones toman forma digital y se transportan a través de redes de telecomunicaciones globales utilizando una combinación de los caminos más rápidos y más baratos sin ninguna referencia significativa a las fronteras nacionales. La vigilancia que no está dirigida directamente a las personas tiene, por tanto, la capacidad de tener un alcance muy amplio, tanto dentro como fuera del territorio del Estado de vigilancia. Por tanto, las salvaguardas son fundamentales y, sin embargo, elusivas. A diferencia de la intercepción dirigida, que ha sido objeto de muchas sentencias del Tribunal, y que se utiliza principalmente para la investigación de delitos, la interceptación masiva también se utiliza, tal vez incluso predominantemente, para la recopilación de inteligencia extranjera y la identificación de nuevas amenazas de actores conocidos y desconocidos. Al operar en este ámbito, los Estados Contratantes tienen una necesidad legítima de mantener el secreto, lo que significa que poco o nada de la información sobre el funcionamiento de sus sistemas será de dominio público, y la información disponible puede expresarse en terminología que es oscura y puede variar significativamente de un Estado a otro.

323. Si bien las capacidades tecnológicas han aumentado considerablemente el volumen de las comunicaciones que atraviesan Internet, las amenazas a las que se enfrentan los Estados Contratantes y sus ciudadanos también han proliferado. Éstas incluyen, entre otras, el terrorismo global, el narcotráfico, la trata de personas y la explotación sexual de niños. Muchas de estas amenazas provienen de redes internacionales de actores hostiles con acceso a una cada vez más sofisticada tecnología que les permite comunicarse sin ser detectados. El acceso a dicha tecnología también permite que agentes estatales y no estatales hostiles alteren la infraestructura digital e incluso el correcto funcionamiento de los procesos democráticos mediante el uso de ciberataques, una seria amenaza para la seguridad que por definición existe solo en el dominio digital y como tal solo se puede detectar e investigar allí. En consecuencia, se solicita al Tribunal que lleve a cabo la evaluación de los regímenes de interceptación masiva de los Estados Contratantes, una valiosa facultad tecnológica para identificar nuevas amenazas en el dominio digital, sobre el cumplimiento del Convenio por referencia a la existencia de salvaguardas contra la arbitrariedad y el abuso, sobre la base de la limitada información sobre la forma en que operan esos regímenes.

(b) La existencia de una interferencia

324. El Gobierno no discute que ha habido una injerencia en los derechos del artículo 8 de los demandantes, aunque alegaron que a efectos del artículo 8 del Convenio, la única injerencia significativa podía haber ocurrido cuando se seleccionaron las comunicaciones para su examen.

325. El Tribunal considera la interceptación masiva como un proceso gradual en el que el grado de injerencia en los derechos del artículo 8 de las personas aumenta a medida que el proceso avanza. Es posible que no todos los regímenes de interceptación masiva sigan exactamente el mismo modelo, y las diferentes etapas del proceso no necesariamente serán diferenciadas o seguidas en estricto orden cronológico. Sin embargo, con sujeción a las salvedades antes mencionadas, el Tribunal considera que a las etapas del proceso de interceptación que deben considerarse se pueden describir de la siguiente manera:

> (a) la interceptación y retención inicial de las comunicaciones y datos relacionados con las comunicaciones (es decir, los datos del tráfico pertenecientes a las comunicaciones interceptadas);
>
> (b) la aplicación de selectores específicos a las comunicaciones / datos relacionados con las comunicaciones;
>
> (c) el examen de las comunicaciones seleccionadas / datos relacionados con las comunicaciones seleccionados por analistas; y
>
> (d) la conservación posterior de los datos y el uso del "producto final", incluido el intercambio de datos con terceros.

326. En lo que el Tribunal ha considerado como la primera etapa, las comunicaciones (o "paquetes" de comunicaciones electrónicas) son interceptadas en masa por los servicios de inteligencia. Estas comunicaciones pertenecen a un gran número de individuos, muchos de los cuales no serán de interés alguno para los servicios de inteligencia. Algunas comunicaciones que probablemente no sean de interés para los servicios de inteligencia pueden filtrarse en esta etapa.

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

328. En lo que el Tribunal ha considerado como la tercera etapa, el material interceptado es examinado por primera vez por un analista.

329. Lo que el Tribunal ha considerado como etapa final es cuando la intercepción del material es realmente utilizada 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.

330. El Tribunal considera que el artículo 8 se aplica a cada una de estas etapas. Mientras que la intercepción inicial seguida por el descarte inmediato de parte de las

comunicaciones no constituye un factor particularmente significativo de interferencia, el grado de interferencia con los derechos del artículo 8 de las personas aumenta a medida que avanza el proceso de interceptación masiva. En este sentido, el Tribunal ha declarado claramente que incluso el mero almacenamiento de datos relacionados con la vida privada de un individuo equivale a una interferencia en el sentido del artículo 8 (véase el asunto *Leander contra Suecia*, 26 de marzo de 1987, § 48, Serie A Núm. 116), y que la necesidad de salvaguardas será mayor cuando se refiere a la protección de los datos personales sometidos a un tratamiento automatizado (ver el asunto *S. y Marper*, antes citada, § 103). El hecho de que el material almacenado lo sea de forma codificada, inteligible solo con el uso de tecnología informática y capaz de ser interpretado sólo por un número limitado de personas, no guarda relación con esa conclusión (véase el asunto *Amann c. Suiza* [GC], núm. 27798/95, § 69, TEDH 2000-II y *S. y Marper*, antes citada, §§ 67 y 75). Finalmente, al final del proceso, cuando la información sobre una persona en particular es analizada o el contenido de las comunicaciones está siendo examinado por un analista, la necesidad de aplicar salvaguardas será máxima. Este enfoque del Tribunal está en consonancia con la conclusión 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 se producía cuando los datos personales almacenados eran procesados y / o a se accedía a ellos por las agencias (véase el párrafo 196 anterior).

331. Por lo tanto, el grado de injerencia en los derechos de privacidad aumentará a medida que el proceso pasa por las diferentes etapas. Al examinar si estaba justificada la creciente interferencia, 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.

(c) Si la interferencia estaba justificada.

(i) Principios generales relacionados con las medidas secretas de vigilancia, incluida la interceptación de comunicaciones

332. Cualquier injerencia en los derechos del artículo 8 de una persona solo puede justificarse en virtud de lo previsto en el artículo 8.2 si es conforme con la ley, persigue uno o más de los objetivos legítimos a los que se refiere ese párrafo y es necesaria en una sociedad democrática para lograr alguno de esos objetivos (ver el asunto *Roman Zakharov*, antes citada, § 227; ver también el asunto *Kennedy contra los Estados* Reino, núm. 26839/05, § 130, de 18 de mayo de 2010). La mención "de acuerdo con la ley" requiere que la medida impugnada tenga alguna base en el derecho interno (a diferencia de una práctica que no tiene una específica base legal- ver el asunto *Heglas c. la República Checa*, núm. 5935/02, § 74, 1 de marzo de 2007-). También debe ser compatible con el estado de derecho, que está expresamente mencionado en el Preámbulo del Convenio y es inherente al objetivo y al objeto del artículo 8. Por tanto, la ley debe ser accesible a las personas afectadas y previsible en cuanto a sus efectos (ver el asunto *Roman Zakharov*, citada arriba, § 228; ver también, entre otras muchas, *Rotaru*, citada anteriormente, § 52; *S. y Marper*, antes citada, § 95, y *Kennedy*, antes citada, § 151).

333. El significado de "previsibilidad" en el contexto de la vigilancia secreta no es el mismo que en muchos otros campos. En el contexto especial de medidas secretas de vigilancia, como la interceptación de comunicaciones, "previsibilidad" no puede

significar que los individuos deben ser capaces de prever cuándo es probable que las autoridades recurran a tales medidas para poder adaptar su conducta en consecuencia. Sin embargo, especialmente cuando un poder conferido al ejecutivo se ejerce en secreto, los riesgos de arbitrariedad son evidentes. Por lo tanto, es esencial contar con reglas claras y detalladas sobre las medidas de vigilancia secreta, especialmente porque la tecnología disponible para su uso es cada vez más sofisticada. El derecho interno debe ser lo suficientemente claro para dar a los ciudadanos una indicación adecuada de las circunstancias y las condiciones en las que las autoridades públicas están facultadas para recurrir a cualquiera de tales medidas (ver *Roman Zakharov*, citada anteriormente, § 229; ver también *Malone*, citada anteriormente, § 67; *Leander*, citada anteriormente, § 51; Huvig, citada anteriormente, § 29; Kruslin, citada anteriormente, § 30; *Valenzuela Contreras c. España*, 30 de julio de 1998, § 46, *Informes de Sentencias y Decisiones* 1998-V; *Rotaru*, citada anteriormente,§ 55; *Weber y Saravia*, antes citada, § 93; y *Asociación para la Unión Europea Integración y Derechos Humanos y Ekimdzhiev c. Bulgaria*, núm. 62540/00, § 75, 28 de junio de 2007). Además, la ley debe indicar el alcance de cualquier facultad discrecional conferida a las autoridades competentes y la forma de ejercerla con suficiente claridad para dar al individuo la protección adecuada contra injerencias arbitrarias (ver *Roman Zakharov*, citada arriba, § 230; ver también, entre otras, *Malone*, citada anteriormente, § 68; *Leandro*, citada anteriormente, § 51; *Huvig*, citada anteriormente, § 29; *Kruslin*, citada anteriormente, § 30; y *Weber y Saravia*, antes citada, § 94).

334. En los casos en los que la legislación que permite la vigilancia secreta sea impugnada ante el Tribunal, la licitud de la injerencia está estrechamente relacionada con la cuestión de si se ha cumplido con el test de "necesidad" por lo que conviene que el Tribunal aborde conjuntamente los requisitos "de conformidad con la ley" y de "necesidad". La "calidad de la ley" en este sentido implica que el derecho interno no solo debe ser accesible y previsible en su aplicación, sino que también debe asegurar que las medidas de vigilancia secretas se aplican sólo cuando "es necesario en una sociedad democrática", en particular, proporcionando salvaguardas y garantías adecuadas y efectivas contra el abuso (ver *Roman Zakharov*, citada anteriormente, § 236; ver también *Kennedy*, citada anteriormente, § 155).

335. Al respecto conviene reiterar que 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 sus comunicaciones sean interceptadas; (iii) un límite en 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 (ver *Huvig*, citada arriba, § 34; *Kruslin*, citada anteriormente, § 35; *Valenzuela Contreras*, antes citada, § 46; *Weber y Saravia*, antes citada, § 95; y *Asociación para la Unión Europea Integración y Derechos Humanos y Ekimdzhiev*, antes citada, § 76). En *Roman Zakharov* (citada anteriormente, § 231) el Tribunal confirmó que las mismas seis salvaguardas mínimas también se aplicaban en los casos en que la interceptación era por razones de seguridad nacional; sin embargo, al determinar si la legislación impugnada violaba el artículo 8, también tomó en cuenta las disposiciones para supervisar la

implementación de medidas de vigilancia secreta, cualesquiera mecanismos de notificación y los recursos previstos por la legislación nacional (ver *Roman Zakharov*, antes citada, § 238).

336. La revisión y supervisión de las medidas de vigilancia secreta puede producirse en tres etapas: cuando se ordena por primera vez la vigilancia, mientras que se está llevando a cabo, o después de que se haya terminado. En cuanto a las dos primeras etapas, la naturaleza y la lógica de la vigilancia secreta dictan que no sólo la vigilancia en sí, sino también la revisión que la acompaña se realice sin el conocimiento del individuo. En consecuencia, dado que el individuo está necesariamente impedido de buscar un remedio efectivo por su propia cuenta o de participar directamente en cualquier procedimiento de revisión, es esencial que los procedimientos establecidos proporcionen por sí mismos garantías equivalentes para salvaguardar sus derechos. En un campo donde el abuso en casos individuales es potencialmente tan fácil y podría tener consecuencias tan dañinas para la sociedad democrática en su conjunto, el Tribunal ha sostenido que en principio, es deseable confiar el control de la supervisión a un juez, el control judicial ofrece las mejores garantías de independencia, imparcialidad y el procedimiento adecuado (ver *Roman Zakharov*, citada anteriormente, § 233; ver también *Klass y otros contra Alemania*, 6 de septiembre de 1978, §§ 55 y 56, Serie A núm. 28).

337. En cuanto a la tercera etapa, una vez finalizada la vigilancia, la cuestión de la notificación posterior de las medidas de vigilancia es un factor relevante para evaluar la efectividad de los recursos antes los tribunales y, por tanto, la existencia de salvaguardas efectivas contra el abuso de los poderes de vigilancia. En principio, hay poco margen para recurrir a los tribunales por el individuo en cuestión, a menos que este último sea informado de la medidas tomadas sin su conocimiento y, por lo tanto, capaz de cuestionar su legalidad retrospectivamente (ver asunto el *Roman Zakharov*, citada anteriormente, § 234; ver también el asunto *Klass y otros*, antes citada, § 57, y *Weber y Saravia*, citada anteriormente, § 135) o, alternativamente, si cualquier persona sospecha que ha sido objeto de vigilancia pueda recurrir a los tribunales, cuya jurisdicción no depende de la notificación al sujeto de las medidas de vigilancia tomadas (ver *Roman Zakharov*, citada anteriormente, § 234; ver también *Kennedy*, citada anteriormente, § 167).

338. En cuanto a la cuestión de si una injerencia era “necesaria en una sociedad democrática” en pos de un fin legítimo, el Tribunal ha reconocido que las autoridades nacionales gozan de un amplio margen de apreciación a la hora de elegir cuál es la mejor manera de lograr el legítimo objetivo de proteger la seguridad nacional (ver *Weber y Saravia*, antes citada, § 106).

339. Sin embargo, este margen está sujeto a la supervisión europea que abarca tanto la legislación como las decisiones que la apliquen. En vista del riesgo de que un sistema de vigilancia secreta establecido para proteger la seguridad nacional (y otros intereses nacionales) pueda socavar o incluso destruir el buen funcionamiento de los procesos democráticos bajo el manto de su defensa, el Tribunal debe cerciorarse de que existen garantías adecuadas y efectivas contra los abusos. La evaluación depende de todas las circunstancias del caso, como la naturaleza, alcance y duración de las posibles medidas, los motivos exigidos para ordenarlas, las autoridades competentes para autorizarlas, ejecutarlas y supervisarlas y el tipo de recurso previsto por la legislación nacional. El

Tribunal debe determinar si los procedimientos para supervisar la orden y la implementación de las medidas restrictivas son capaces de limitar la "interferencia" a lo que es "necesario en una sociedad democrática" (ver *Roman Zakharov*, antes citada, § 232; véase también *Klass y otros*, antes citada, §§ 49, 50 y 59, *Weber y Saravia*, antes citada, § 106 y *Kennedy*, citada anteriormente, §§ 153 y 154).

(ii) Sobre si es necesario desarrollar la jurisprudencia

340. En los asuntos *Weber y Saravia* y *Liberty y otros* (antes citados) el Tribunal aceptó que los regímenes de interceptación masiva no se encontraban *per se* fuera del margen de apreciación de los Estados. Ante la proliferación de amenazas a las que los Estados se enfrentan actualmente por redes de actores internacionales, que utilizan Internet tanto para la comunicación así como de herramienta, y la existencia de tecnología sofisticada que permitiría a estos actores evitar la detección (ver párrafo 323 anterior), el Tribunal considera que la decisión de operar un régimen de interceptación masiva con el fin de identificar amenazas a la seguridad nacional o en contra de los intereses nacionales esenciales sigue cayendo dentro de este margen.

341. En los asuntos *Weber y Saravia* y *Liberty y Otros* (antes citados) el Tribunal aplicó las seis salvaguardas mínimas antes mencionadas desarrolladas en su jurisprudencia sobre la interceptación selectiva (véase el apartado 335 anterior). Sin embargo, mientras que los regímenes de interceptación masiva considerados en esos casos eran a primera vista similares a los que se discuten en el presente caso, ambos casos tienen ahora más de diez años, y en los años que han transcurrido los desarrollos tecnológicos han cambiado significativamente la forma en que las personas se comunican. Las vidas se viven cada vez más *on line*, generando por tanto un volumen significativamente mayor de comunicaciones electrónicas, y comunicaciones de naturaleza y calidad significativamente diferentes, a aquéllas que probablemente se generaran hace una década (véase el párrafo 322 anterior). El alcance de la actividad de vigilancia considerada en esos casos, por lo tanto, ha sido mucho más limitado.

342. Lo mismo ocurre con los datos relacionados con las comunicaciones. Como el ISR observó en su informe, en la actualidad se encuentra disponible un mayor volumen de datos de comunicaciones en relación con un individuo que de contenido, ya que cada pieza de contenido está rodeada de múltiples piezas de datos de las comunicaciones (véase el párrafo 159 anterior). Si bien el contenido puede estar cifrado y, en cualquier caso, puede no revelar cuestiones importantes sobre el remitente o el destinatario, los datos relacionados con las comunicaciones pueden 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 relacionados con las comunicaciones se ampliará cuando se obtengan de forma masiva, ya que permiten ser analizados e interrogados para pintar el cuadro íntimo de una persona a través del mapeo de redes sociales, rastreo de ubicación, seguimiento de la navegación en Internet, mapeo de patrones de comunicación y el conocimiento sobre con quién interactuó una persona (ver el párrafo 317 anterior).

343. Y lo que es más importante, en *Weber y Saravia* y *Liberty y Otros* el Tribunal no abordó expresamente el hecho de que se trataba de una vigilancia de diferente

naturaleza y escala a la considerada en casos anteriores. No obstante, la interceptación dirigida y la intercepción masiva son diferentes en varios aspectos importantes.

344. Para empezar, la interceptación masiva generalmente se dirige a comunicaciones internacionales (es decir, comunicaciones que viajan físicamente a través de las fronteras estatales), y si bien la interceptación e incluso el examen de las comunicaciones de personas dentro del Estado vigilante pueden no estar excluidas, en muchos casos el fin declarado de la interceptación masiva es vigilar las comunicaciones de personas ajenas a la jurisdicción territorial del Estado, que no podrían ser monitoreadas mediante otras formas de vigilancia. Por ejemplo, el sistema alemán solo tiene como objetivo monitorear telecomunicaciones fuera del territorio alemán (véase el párrafo 248 anterior). En Suecia, el material de interceptación no puede relacionarse con señales en las que tanto el remitente como el destinatario se encuentran en Suecia (véase la sentencia de hoy en el caso de *Centrum för rättvisa contra Suecia* (demanda núm. 35252/08)).

345. Además, como ya se ha señalado, los fines para los que se ha empleado la interceptación masiva parecen ser diferentes. El Tribunal ha considerado que la interceptación dirigida, en su mayor parte, ha sido empleada por los Estados demandados con el fin de investigar un delito. Sin embargo, aunque la intercepción masiva puede usarse para investigar ciertos delitos, los Estados miembros del Consejo de Europa que emplean regímenes de interceptación masiva parecen utilizarlos para fines de recopilación de inteligencia extranjera, la detección e investigación precoces de ciberataques, contraespionaje y lucha contra el terrorismo (véanse los párrafos 303, 308 y 323 anteriores).

346. Si bien la interceptación masiva no se usa necesariamente para vigilar a individuos específicos, evidentemente puede ser - y es - usada para este fin. Sin embargo, cuando este es el caso, los dispositivos de las personas objetivo no se monitorean. Más bien, los individuos se convierten en el "objetivo" mediante la aplicación de selectores fuertes (como sus direcciones de correo electrónico) a las comunicaciones interceptadas en masa por los servicios de inteligencia. Solo esos "paquetes" de comunicaciones de las personas objetivo que viajaban a través de los portadores seleccionados por los servicios de inteligencia habrán sido interceptados de esta manera, y sólo aquellas comunicaciones interceptadas que coincidían con un selector fuerte o una consulta compleja podrán ser examinadas por un analista.

347. Como ocurre con cualquier régimen de interceptación, existe, por supuesto, un riesgo potencial considerable de que se abuse de la interceptación masiva de una manera que afecte negativamente al derecho de las personas al respeto de la vida privada. Si bien el artículo 8 del Convenio no prohíbe el uso de la intercepción masiva para proteger la seguridad y otros intereses nacionales esenciales frente a graves amenazas, y los Estados disfrutan de un amplio margen de apreciación al decidir qué tipo de régimen de interceptación es necesario, a estos efectos, para el funcionamiento de tal sistema, el margen de apreciación que se les concede debe ser más estrecho y deberán estar presentes una serie de salvaguardas. El Tribunal ya identificó las salvaguardas que deberían figurar en un régimen de interceptación dirigida. Si bien esos principios proporcionan un marco útil para este ejercicio, deberán adaptarse para reflejar las características específicas de un régimen de interceptación masiva y, en particular, los

crecientes grados de intrusión en los derechos del artículo 8 de las personas conforme se avanza en las etapas identificadas en el párrafo 325 anterior.

(iii) El enfoque a seguir en los casos de interceptación masiva.

348. Es claro que las dos primeras de las seis "salvaguardas mínimas" que el Tribunal, en el contexto de la interceptación dirigida, ha establecido que deben ser definidas claramente en la legislación interna para evitar abusos de poder (estas son, la naturaleza de las infracciones que pueden dar lugar a una orden de interceptación y las categorías de personas cuyas comunicaciones pueden ser interceptadas: véase párrafo 335 anterior), no son fácilmente aplicables a un régimen de interceptación masiva. Asimismo, el requisito de "sospecha razonable", que podemos encontrar en la jurisprudencia del Tribunal sobre la interceptación selectiva en el contexto de investigaciones criminales es menos pertinente en el contexto de interceptación masiva, cuya finalidad es en principio preventiva, más que para la investigación de un objetivo específico y/o un delito penal identificable. Sin embargo, el Tribunal considera imperativo que cuando un Estado está operando tal régimen, la legislación nacional contenga normas detalladas sobre cuándo las autoridades pueden recurrir a tales medidas. En particular, la legislación nacional debe establecer con suficiente claridad los motivos por los cuales la interceptación masiva puede ser autorizada y las circunstancias en las que las comunicaciones de un individuo pueden ser interceptadas. Las cuatro salvaguardas mínimas restantes definidas por el Tribunal en sus sentencias anteriores -es decir, que el derecho interno debe establecer un límite en la duración de la interceptación, el procedimiento a seguir para examinar, utilizar y almacenar los datos obtenidos, las precauciones que deben tomarse al comunicar los datos a terceros, y las circunstancias en las cuales los datos interceptados pueden o deben ser borrados o destruidos- son igualmente pertinentes en cuanto a la interceptación masiva.

349. En su jurisprudencia sobre la interceptación selectiva, el Tribunal ha tenido en cuenta las disposiciones para la supervisión y revisión del régimen de interceptación (*ver Roman Zakharov*, citada anteriormente, §§ 233-234). En el contexto de la interceptación masiva se amplifica la importancia de la supervisión y revisión, por el riesgo inherente de abuso y por la legítima necesidad de secreto que implica inevitablemente que, por razones de seguridad nacional, los Estados a menudo no tengan la libertad de revelar información sobre el funcionamiento del régimen impugnado.

350. Por lo tanto, para minimizar el riesgo de abuso de poder en la intercepción masiva, el Tribunal considera que el proceso debe estar sujeto a "salvaguardas de extremo a extremo", lo que significa que, a nivel interno, debe hacerse una evaluación en cada etapa del proceso acerca de la necesidad y proporcionalidad de las medidas que se toman; que la intercepción masiva debe estar sujeta a autorización independiente desde el principio, cuando el objeto y alcance de la operación se están definiendo; y que la operación debe estar sujeta a una supervisión y revisión independiente *ex post facto*. En opinión del Tribunal, estas son garantías fundamentales que constituyen la piedra angular de cualquier régimen de interceptación masiva conforme al artículo 8 (véase también el informe del Comisión de Venecia, en el párrafo 197 anterior, que de manera similar concluyó que dos de las salvaguardas más importantes en un régimen de interceptación masiva eran la autorización y la supervisión del proceso).

351. Comenzando por la autorización, la Gran Sala coincide con la Sala en que si bien la autorización judicial es una "salvaguarda importante contra a la arbitrariedad" no es un "requisito necesario" (ver párrafos 318-320 de la sentencia de la Sala). Sin embargo, la intercepción masiva debe ser autorizada por un organismo independiente; es decir, por un organismo que sea independiente del ejecutivo.

352. Además, a fin de proporcionar una salvaguarda eficaz contra el abuso, el organismo independiente que conceda la autorización debe ser informado tanto del fin de la interceptación como de los portadores o rutas de comunicación que probablemente sean interceptadas. Esto permitiría a dicho organismo evaluar la necesidad y la proporcionalidad de la operación de interceptación masiva y también evaluar si la selección de portadores es necesaria y proporcionada en relación con los fines para los que se realiza la interceptación.

353. El uso de selectores - y de selectores fuertes en particular- es uno de los pasos más importantes en el proceso de interceptación masiva, ya que este es el punto en el que la interceptación de las comunicaciones de un individuo en particular puede ser dirigida por los servicios de inteligencia. Sin embargo, aunque algunos sistemas permiten la previa autorización del uso de categorías de selectores (ver, por ejemplo, el sistema sueco descrito en detalle en la sentencia *Centrum för rättvisa c. Suecia* (demanda núm. 35252/08)), el Tribunal observa que los Gobiernos de Reino Unido y los Países Bajos han alegado que cualquier requisito relativo a explicar o fundamentar los selectores o los criterios de búsqueda en la autorización restringiría gravemente la efectividad de la interceptación masiva (véanse los párrafos 292 y 307 anteriores). Este argumento fue acogido por el IPT, que consideró que "la inclusión de los selectores en la autorización podía socavar y limitar innecesariamente el funcionamiento de la orden y ser en todo caso completamente irreal" (ver párrafo 49 anterior).

354. Teniendo en cuenta las características de la interceptación masiva (ver párrafos 344 a 345 anteriores), el gran número de selectores empleados y la necesidad inherente de flexibilidad en la elección de los selectores, que en la práctica pueden expresarse como combinaciones técnicas de números o letras, el Tribunal debe aceptar que la inclusión de todos los selectores en la autorización no sea factible en la práctica. No obstante, dado que la elección de los selectores y los términos de consulta determinan qué comunicaciones serán elegibles para su examen por un analista, la autorización debe al menos identificar los tipos o categorías de selectores que se utilizarán.

355. Además, deben establecerse salvaguardas mejoradas 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 la justificación debe registrarse escrupulosamente y estar sujeta a un proceso de autorización interna previa llevado a cabo por separado y una verificación objetiva acerca de si la justificación se ajusta a los principios antes mencionados.

356. Cada etapa del proceso de interceptación masiva - incluida la autorización inicial y las renovaciones posteriores, la selección de los portadores, la elección y aplicación de selectores y términos de consulta, y el uso, almacenamiento, ulterior transmisión y eliminación del material interceptado - también debe estar sujeta a la supervisión de una autoridad independiente y la supervisión debe ser lo suficientemente sólida para

mantener la "interferencia" a aquello que sea "necesario en una sociedad democrática" (ver *Roman Zakharov*, citada anteriormente,§ 232; ver también *Klass y otros*, antes citada, §§ 49, 50 y 59; *Weber y Saravia*, antes citada, § 106 y *Kennedy*, antes citada, §§ 153 y 154). En particular, el organismo supervisor debe estar en condiciones de evaluar la necesidad y proporcionalidad de la acción que se está adoptando, teniendo en cuenta el nivel correspondiente de intromisión en los derechos del Convenio de las personas que puedan verse afectadas. Para facilitar esta supervisión, los servicios de inteligencia deben mantener registros detallados de cada etapa del proceso.

357. Por último, debe estar disponible un recurso efectivo para cualquier persona que sospeche que sus comunicaciones han sido interceptadas por los servicios de inteligencia, ya sea para impugnar la legalidad de la interceptación o el cumplimiento del Convenio por el régimen de interceptación. En el contexto de la interceptación selectiva, el Tribunal ha establecido repetidamente que la subsiguiente notificación de las medidas de vigilancia es un factor relevante para asegurar la eficacia de los recursos ante los tribunales y de ahí deriva la existencia de salvaguardas eficaces contra el abuso en los poderes de vigilancia. De todos modos, se ha reconocido que la notificación no es necesaria si el sistema de recursos internos permiten a cualquier persona que sospeche que sus comunicaciones están siendo o han sido interceptadas dirigirse a los tribunales; en otras palabras, cuando la jurisdicción de los tribunales no depende de la notificación al sujeto de la interceptación de que ha habido una interceptación de su comunicaciones (ver *Roman Zakharov*, citada anteriormente, § 234 y Kennedy, citada anteriormente, § 167).

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

359. Las facultades y garantías procesales que posee una autoridad son relevantes para determinar si un recurso es efectivo. Por lo tanto, en ausencia del requisito de la notificación, es imperativo que el recurso deba plantearse ante un organismo que, si bien no sea necesariamente judicial, sea independiente del ejecutivo y asegure la equidad en el procedimiento, ofreciendo, en la medida en que sea posible, un proceso contradictorio. Las decisiones de dicha autoridad serán razonadas y jurídicamente vinculantes con respecto, entre otras cuestiones, al cese de la interceptación ilícita y la destrucción de las obtenidas ilícitamente y / o del material interceptado almacenado (ver, *mutatis mutandis*, *Segerstedt-Wiberg y Otros contra Suecia*, núm. 62332/00, § 120, TEDH 2006-VII y también *Leander*, citada anteriormente, §§ 81-83 donde la falta de poder para adoptar una decisión legal vinculante constituyó la debilidad principal del control ofrecido).

360. A la luz de lo anterior, el Tribunal determinará si un régimen de interceptación cumple con el Convenio mediante la realización de una evaluación del funcionamiento de dicho régimen. Dicha evaluación se centrará principalmente en si el marco legal interno contiene suficientes garantías contra el abuso, y en si el proceso está sujeto a "salvaguardas de extremo a extremo" (véase el párrafo 350 anterior). Al hacerlo, tendrá en cuenta el funcionamiento real del sistema de interceptación, incluidos los controles y equilibrios sobre el ejercicio del poder, y la existencia o ausencia de cualquier evidencia de abuso real (ver *Asociación para la Integración Europea y los Derechos Humanos y Ekimdzhiev*, antes citada, § 92).

361. Al evaluar si el Estado demandado actuó dentro de su margen de apreciación (véase el párrafo 347 anterior), el Tribunal tendrá que tener en cuenta una gama más amplia de criterios que las seis salvaguardas del asunto *Weber*. Más específicamente, al abordar conjuntamente los requisitos "de conformidad con la ley" y de "necesidad" como el enfoque establecido en esta materia (ver *Roman Zakharov*, citada anteriormente, § 236 y *Kennedy*, citada anteriormente, § 155), el Tribunal examinará si el marco legal nacional definía claramente:

1. los motivos por los que se puede autorizar la interceptación masiva;

2. las circunstancias en las que las comunicaciones de un individuo pueden ser interceptadas;

3. el procedimiento a seguir para la concesión de la autorización;

4. los procedimientos a seguir para seleccionar, examinar y utilizar el material interceptado;

5. las precauciones que deben tomarse 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 de supervisión por una autoridad independiente del cumplimiento de las salvaguardas anteriores y sus poderes para abordar el incumplimiento;

8. los procedimientos para la revisión independiente *ex post facto* de tales cumplimientos y las facultades conferidas al órgano competente para abordar casos de incumplimiento.

362. A pesar de ser uno de los seis criterios de *Weber*, hasta la fecha el Tribunal aún no ha proporcionado orientación específica sobre las precauciones que deben tomarse al comunicar el material interceptado a otras partes. Sin embargo, ahora es claro que algunos Estados están compartiendo 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 del material obtenido mediante intercepción masiva debe limitarse al material que haya sido recopilado y almacenado de una forma que cumpla con el Convenio y debe estar sujeto a ciertas salvaguardas específicas adicionales relativas a la

transferencia en sí. En primer lugar, las circunstancias en las que puede tener lugar tal transferencia deben establecerse claramente en la legislación nacional. En segundo lugar, el Estado que transfiere debe asegurarse de que el Estado receptor, al tramitar los datos, cuenta con medidas de seguridad capaces de prevenir el abuso y una interferencia desproporcionada. En particular, el Estado receptor debe garantizar el almacenamiento seguro del material y restringir su posterior divulgación. Esto no significa necesariamente que el Estado receptor deba gozar de una protección comparable a la del Estado que transfiere; ni que éste necesariamente deba asegurarse de que se den las garantía antes de cada transferencia. En tercer lugar, será necesario reforzar las salvaguardas cuando esté claro que el material que se está transfiriendo requiere de una especial confidencialidad - como el material periodístico confidencial–. Finalmente, el Tribunal considera que la transferencia de material a socios de inteligencia extranjeros también debe estar sujeta a un control independiente.

363. Por las razones identificadas en el párrafo 342 anterior, el Tribunal no considera que la adquisición de datos relacionados con las comunicaciones a través de la interceptación sea necesariamente menos intrusiva que la adquisición de contenido. Por tanto, considera que la interceptación, retención y búsqueda de los datos relacionados con las comunicaciones deben analizarse con referencia a las mismas salvaguardas que las aplicables al contenido.

364. Dicho esto, mientras que la interceptación de los datos relacionados con las comunicaciones normalmente se autorizará al mismo tiempo que la interceptación del contenido, una vez obtenidos pueden ser tratados de manera diferente por los servicios de inteligencia (véanse, por ejemplo, los párrafos 153 a 154 anteriores). En vista del diferente carácter de los datos relacionados con las comunicaciones y las diferentes formas en que son utilizados por los servicios de inteligencia, siempre que se den las salvaguardas antes mencionadas, el Tribunal considera que las disposiciones legales que rigen su tratamiento no necesariamente tienen que ser idénticas en todos los aspectos a las que rigen el tratamiento del contenido.

(iv) La evaluación del Tribunal del caso en cuestión

(1) Observaciones preliminares

365. En el momento que nos concierne la interceptación masiva tenía su base jurídica en el Capítulo I de la RIPA. Además, el Tribunal considera que dicho régimen perseguía los objetivos legítimos de proteger la seguridad nacional, prevenir el desorden y la delincuencia y la protección de los derechos y libertades de los demás. Por lo tanto, siguiendo el enfoque esbozado en el párrafo 334 anterior, queda por considerar si la legislación nacional era accesible y contenía salvaguardas adecuadas y efectivas para cumplir con los requisitos de "previsibilidad" y "necesidad en una sociedad democrática".

366. Las disposiciones legislativas pertinentes que regían el funcionamiento de los regímenes de interceptación masiva eran indudablemente complejas; de hecho, la mayoría de los informes sobre los regímenes de vigilancia secreta del Reino Unido criticaban su falta de claridad (véanse los párrafos 143, 152 y 157 anteriores). Sin embargo, esas disposiciones se aclararon en el Código de prácticas de intercepción de comunicaciones ("el Código IC" - véase el párrafo 96 anterior-). El párrafo 6.4 del Código IC dejó claro que la interceptación masiva estaba teniendo lugar y proporcionó

más detalles de cómo este particular régimen de vigilancia era aplicado en la práctica (véase el párrafo 96 anterior). El Código IC es un documento público aprobado por ambas Cámaras del Parlamento, que es publicado por el Gobierno *on line* y en versión impresa, y que debe ser tenido en cuenta tanto por las personas que ejercen funciones de interceptación como por los tribunales (véanse los párrafos 93 a 94 anteriores). En consecuencia, esta Tribunal aceptó que sus disposiciones podían tenerse en cuenta al evaluar la previsibilidad de la RIPA (ver *Kennedy*, citada anteriormente, § 157). En consecuencia, el Tribunal considera que el derecho interno era suficientemente "accesible".

367. Pasando a la cuestión de si la ley contenía salvaguardas y garantías efectivas para cumplir con los requisitos de "previsibilidad" y "necesidad en una sociedad democrática", el Tribunal abordará en la subsección (β) cada uno de los ocho requisitos establecidos en el párrafo 361 anterior con respecto a la interceptación del contenido de las comunicaciones electrónicas. En la subsección (γ) examinará más específicamente la interceptación de los datos relacionados con las comunicaciones.

(2) Interceptación del contenido de las comunicaciones

- 1. Motivos por los que se puede autorizar la interceptación masiva.

368. Bajo la sección 5(3) de la RIPA y el párrafo 6.11 del Código IC (ver párrafos 62 y 96 anteriores), el Secretario de Estado sólo podía emitir una orden de intercepción si él o ella estaba convencido de que era necesaria en intereses de la seguridad nacional, con el fin de prevenir o detectar delitos graves, o con el fin de salvaguardar el bienestar económico del Reino Unido en la medida en que esos intereses también fueran necesarios para el mantenimiento de la seguridad nacional.

369. Estos motivos estaban sujetos a las siguientes limitaciones. Ante todo, el Comisionado IC había aclarado que en la práctica la "seguridad nacional" permitía actividades de la vigilancia cuando se amenazaba la seguridad o el bienestar del Estado y de las actividades encaminadas a socavar o derrocar la democracia parlamentaria por medios políticos, industriales o violentos (ver *Kennedy*, citada anteriormente, § 333). En segundo lugar, el delito grave se definió en artículo 81(2)(b) de la RIPA como un delito por el cual el perpetrador (suponiendo que era mayor de veintiún años y no tenía antecedentes penales) podía esperar razonablemente ser condenado a una pena de prisión de tres años o más; o cuando la conducta involucraba el uso de la violencia, resultaba en una ganancia financiera sustancial o era realizada por un gran número de personas que perseguían un fin común (véase el párrafo 63 anterior). En tercer lugar, la sección 17 de la RIPA y el párrafo 8.3 del Código IC disponían que, como regla general ni la posibilidad de interceptación, ni el material interceptado en sí mismo, podían desempeñar papel alguno en los procesos judiciales (véanse los párrafos 83 y 96 anteriores). Por lo tanto, aunque la interceptación podía utilizarse con fines de prevención o detección de delitos graves, no se podía utilizar el material interceptado en la persecución de un delito penal. Además, el párrafo 6.8 del Código IC dispuso que el fin de una orden de la sección 8(4) debía "reflejar típicamente una o más de las prioridades de inteligencia establecidas por el Consejo de Seguridad Nacional" (véanse los párrafos 96 y 98 anteriores).

370. En principio, cuanto más amplios sean los motivos, mayor será el potencial riesgo de abuso. Sin embargo, motivos más delimitados y/o más estrictamente definidos solo

proporcionan una garantía efectiva contra el abuso si se hubieran establecido otras salvaguardas suficientes para asegurar que la interceptación masiva solo se autoriza por un motivo permitido y que era necesaria y proporcionada para tal fin. La cuestión estrechamente relacionada de si existían suficientes garantías para asegurar que la interceptación era necesaria o justificada es, por lo tanto, tan importante como el grado de precisión con el que debe ser definido el motivo en el que se fundamenta la autorización. En consecuencia, desde el punto de vista del Tribunal, un régimen que permite que se ordene la interceptación masiva en base a motivos amplios aún puede cumplir con el artículo 8 del Convenio, siempre que, visto en su conjunto, se construyan suficientes garantías contra el abuso en el sistema para compensar esta debilidad.

371. En el Reino Unido, aunque los motivos por los que se podía autorizar la interceptación se formularon en términos relativamente amplios, se centraban en la seguridad nacional, así como en los delitos graves y el bienestar económico del país en la medida en que esos intereses también fueran relevantes para los intereses de la seguridad nacional (véase el párrafo 368 anterior). Por lo tanto, el Tribunal pasará a considerar las otras garantías integradas en el régimen de la sección 8(4) para determinar si, visto en su conjunto, cumplía con el artículo 8 del Convenio.

– 2. Las circunstancias en las que las comunicaciones de un individuo pueden ser interceptadas.

372. El párrafo 6.2 del Código IC (véase el párrafo 96 anterior) claramente declaró que "[e] n contraste con la sección 8 (1), una orden de la sección 8 (4) no ha de nombrar o describir al sujeto de la interceptación o el conjunto de premisas en relación con las cuales se llevará a cabo la interceptación. Tampoco la sección 8 (4) impone un límite expreso en el número de comunicaciones externas que pueden ser interceptadas". En otras palabras, el objetivo eran los portadores de comunicaciones en lugar de los dispositivos desde los que se enviaron las comunicaciones, o los remitentes o destinatarios de las comunicaciones. En ausencia de cualquier límite en el número de comunicaciones que podían ser interceptadas, parece que todos los paquetes de comunicaciones que fluían a través de los portadores objetivo eran interceptados mientras la orden estaba en vigor.

373. Dicho esto, una orden de la sección 8 (4) era una orden para la interceptación de comunicaciones externas (ver párrafo 72 anterior) y el párrafo 6.7 del Código IC (ver párrafo 96 anterior) requería que la agencia de interceptación que realizara la interceptación bajo una orden de la sección 8 (4) utilizara su conocimiento de la forma en que las comunicaciones internacionales eran enrutadas, combinado con encuestas periódicas de enlaces de comunicaciones relevantes, para identificar aquellos portadores de comunicaciones individuales que tenían más probabilidades de contener comunicaciones externas que cumplieran con la descripción del material certificado por la Secretaría de Estado. También era necesario que la agencia interceptora realizara la intercepción de forma que limitaran la recopilación de comunicaciones no externas al nivel mínimo compatible con el objetivo de interceptar las comunicaciones externas deseadas. Los portadores no eran, por tanto, elegidos al azar. Al contrario, eran seleccionados porque se creía que eran los más propensos para detectar comunicaciones de interés de inteligencia.

374. En el párrafo 6.5 del Código IC se definían las "comunicaciones externas" como las comunicaciones que eran enviadas o recibidas fuera de las Islas Británicas (véase el párrafo 96 anterior). Cuando el remitente y el destinatario estaban dentro de las Islas Británicas, la comunicación era interna. Por lo tanto, que fuera o no una comunicación "externa", dependía de la ubicación geográfica del remitente y del destinatario y no de la ruta que llevaba la comunicación a su destino. Las comunicaciones que cruzaban las fronteras del Reino Unido (comunicaciones internacionales) también podían ser consideradas "internas", ya que una comunicación (o paquetes de comunicaciones) enviada desde y recibida en el Reino Unido, no obstante, podía enrutarse a través de uno o más terceros países.

375. La distinción entre comunicaciones internas y externas no evita, por tanto, la interceptación de comunicaciones internas que viajan a través de las fronteras del Reino Unido y, de hecho, la "captura incidental" de dichas comunicaciones estaba expresamente permitida por la sección 5 (6) de la RIPA, que disponía que la conducta autorizada por una orden de interceptación incluía la interceptación de comunicaciones no identificadas por la orden si era necesario para realizar lo que fue expresamente autorizado por la orden (ver párrafo 68 anterior). Además, la definición de "externa" era en sí misma suficientemente amplia para incluir el almacenamiento en la nube y la navegación y las actividades en redes sociales de una persona en el Reino Unido (véanse los párrafos 75 y 76 anteriores). No obstante, como reconoció la Sala, la salvaguarda de las "comunicaciones externas" tenía un papel que desempeñar en el macro nivel de la selección de los portadores de la interceptación (ver párrafo 337 de la sentencia de la Sala); ya que la agencia interceptora tenía que utilizar su conocimiento de la forma en que las comunicaciones internacionales se enrutaban para identificar esas comunicaciones y los portadores con mayor probabilidad de contener comunicaciones externas de valor para la operación, la salvaguarda, aunque de forma limitada, circunscribía las categorías de personas que podían ver como sus comunicaciones eran interceptadas. También era relevante para la cuestión de la proporcionalidad, ya que los Estados podían tener medidas menos intrusivas a su alcance para obtener las comunicaciones de personas dentro de su jurisdicción territorial.

376. A la luz de lo anterior, el Tribunal considera claro que las comunicaciones internacionales bajo el del régimen de la sección 8 (4) (es decir, comunicaciones que cruzaban las fronteras estatales) podían ser interceptadas; y que los servicios de inteligencia solo usarían su poder para interceptar aquellos portadores con mayor probabilidad de llevar a cabo comunicaciones externas de interés de inteligencia. En el contexto de la interceptación masiva es difícil, en abstracto, imaginar cómo las circunstancias en las que las comunicaciones de un individuo pueden ser interceptadas podían delimitarse aún más. En cualquier caso, como ni el remitente ni el destinatario de una comunicación electrónica podían controlar la ruta que la llevaría a su destino, en la práctica cualquier restricción adicional sobre la elección de los portadores no hubiera hecho más previsible la legislación nacional en cuanto a sus efectos. Por tanto, el Tribunal considera que las circunstancias en las que las comunicaciones de un individuo podían ser interceptadas bajo el régimen de la sección 8 (4) eran suficientemente "previsibles" a los efectos del artículo 8 del Convenio.

- 3. El procedimiento a seguir para la concesión de la autorización

377. Una solicitud de una orden de las previstas en la sección 8(4) era presentada al Secretario de Estado, que era el único que tenía el poder de emitir tal orden. Antes de su presentación, cada solicitud estaba sujeta a una revisión dentro de la agencia que la realizaba. Esto implicaba el escrutinio de más de un funcionario, que tenían que considerar si la solicitud se realizaba para un fin de la sección 5 (3) de la RIPA y si la interceptación propuesta satisfacía los criterios de necesidad y proporcionalidad del Convenio (véase el párrafo 6.9 del el Código IC, en el párrafo 96 anterior). Este nivel adicional de escrutinio interno era sin duda valioso, pero seguía ocurriendo, en el momento que debemos considerar, que la interceptación masiva realizada bajo el régimen de la sección 8 (4) era autorizada por el Secretario de Estado y no por un organismo independiente del ejecutivo. En consecuencia, el régimen de la sección 8 (4) carecía de una de las salvaguardas fundamentales; esto es, que la interceptación masiva debía estar sujeta a una autorización independiente desde el principio (véase el párrafo 350 anterior).

378. En cuanto al nivel de escrutinio proporcionado por el Secretario de Estado, el párrafo 6.10 del Código IC establecía en detalle la información que debía incluirse en la solicitud (véase el párrafo 96 anterior). Ésta incluía una descripción de las comunicaciones a interceptar, detalles del proveedor (es) de servicios de comunicaciones y una evaluación de la viabilidad de la operación, cuando fuera pertinente; una descripción de la conducta a autorizar; el certificado que regularía el examen del material interceptado (ver párrafos 378 y 379 siguientes); una explicación de por qué la interceptación era considerada necesaria para uno o más de los fines de la sección 5 (3); la consideración de por qué la conducta era proporcionada respecto a lo que se pretendía lograr; una garantía de que el material interceptado se leería, examinaría o escucharía solo en la medida en que estuviera certificado y cumpliera las condiciones de secciones 16 (2) a 16 (6) de la RIPA; y una garantía de que el material interceptado se manejaría de acuerdo con las salvaguardas de la sección 15 y la sección 16.

379. En consecuencia, el Secretario de Estado era informado de la finalidad de la operación (que tenía que ser uno de los fines previstos en la sección 5 (3)) y, antes de emitir la orden, tenía que estar convencido de que era necesaria para ese fin, y de que era proporcionada a lo que se buscaba lograr (ver párrafos 6.11 y 6.13 del Código IC en el párrafo 96 anterior). Al evaluar la proporcionalidad, el Secretario de Estado tenía que considerar si la orden era excesiva dadas las circunstancias generales del caso y si la información buscada podía haber sido obtenida razonablemente por medios menos intrusivos (véase el párrafo 3.6 del Código IC en el párrafo 96 anterior). En particular, era necesario equilibrar el tamaño y el alcance de la interferencia frente a lo que se buscaba lograr; había que dar una explicación de cómo y por qué los métodos causarían la menor intrusión posible en el sujeto y en otros; había que considerar si la actividad era una forma adecuada de lograr el resultado necesario, habiendo considerado todas las alternativas razonables; y, en la medida de lo posible, tenían que aportase pruebas de otros métodos considerados pero evaluados como insuficientes para cumplir los objetivos operativos (ver párrafo 3.7 del Código IC en el párrafo 96 anterior).

380. Aunque la solicitud de una orden de las previstas en la sección 8 (4) tenía que incluir “una descripción de las comunicaciones que se van a interceptar” y “detalles del proveedor (es) de servicios de comunicaciones”, el Gobierno confirmó en la vista que la orden no especificaba portadores particulares, porque habría “graves problemas de

impracticabilidad y dificultades" si eso fuera un requisito. Sin embargo, tenía que haber una descripción adecuada de lo que involucraría la interceptación y detalles de la "clase de portadores" que serían interceptados. Esta información permitía al Secretario de Estado la evaluación de la necesidad y proporcionalidad de la conducta descrita en la solicitud. Además, el Gobierno confirmó en sus alegaciones ante la Gran Sala que el Comisionado IC fue informado regularmente por la GCHQ de la base sobre la cual eran seleccionados los portadores para la interceptación (véase el párrafo 290 anterior).

381. La solicitud de una orden de las previstas en la sección 8 (4) tampoco tenía que incluir una indicación de las categorías de selectores que se emplearían. En consecuencia, no había posibilidad de evaluar su necesidad y proporcionalidad en la etapa de autorización, aunque la elección de los selectores a partir de entonces estuviera sujeta a supervisión independiente. En sus alegaciones ante la Gran Sala el Gobierno confirmó que cada vez que se agregaba un nuevo selector al sistema, el analista tenía que completar un registro escrito, explicando por qué era necesario y proporcionado aplicar el selector para los fines incluidos en el certificado del Secretario de Estado. Esto se realizaba mediante la selección de un texto de un menú desplegable, seguido, además, por parte del analista, de un texto libre explicando por qué era necesario y proporcionado para realizar la búsqueda. Además, el uso de selectores tenía que ser registrado en un lugar aprobado que permitiera que fueran auditados; debía crearse un registro de búsqueda de selectores en uso; y ser susceptibles de supervisión por el Comisionado IC (véanse los párrafos 291 a 292 anteriores). La elección de los selectores estaba, por lo tanto, sujeta a la supervisión del Comisionado IC y en su informe anual de 2016 confirmó que "quedó impresionado por la calidad de las declaraciones" preparadas por los analistas que explicaban la necesidad y proporcionalidad al agregar un nuevo selector (véase el párrafo 177 anterior).

382. Dado que la elección de los selectores y los términos de consulta determinaban qué comunicaciones serían elegibles para ser examinadas por un analista, el Tribunal ha señalado que es de fundamental importancia que al menos las categorías de selectores se identificarán en la autorización y para aquellos selectores fuertes vinculados a individuos identificables que estuvieran sujetos a una autorización interna previa que proporcione una verificación separada y objetiva de si la justificación se ajusta a los principios antes mencionados (ver párrafos 353 a 355 anteriores).

383. En el presente caso, la ausencia de supervisión de las categorías de selectores en el momento de la autorización era una deficiencia del régimen de la sección 8 (4). El control posterior de todos los selectores individuales tampoco satisfizo el requisito de salvaguardas mejoradas para el uso de selectores potentes vinculados a personas identificables ni la necesidad de contar con un proceso interno de autorización previa que previera una verificación separada y objetiva de si la justificación se ajustaba a los principios antes mencionados (ver párrafo 355 anterior). Aunque los analistas tuvieron que registrar y justificar el uso de cada selector con respecto a los principios de necesidad y proporcionalidad del Convenio y esa justificación se sometió a la supervisión del Comisionado IC, los selectores fuertes vinculados a personas identificables, sin embargo, no estaban sujetos a autorización interna previa.

- 4. Los procedimientos a seguir para seleccionar, examinar y utilizar el material interceptado.

384. El párrafo 6.4 del Código IC estipulaba que cuando una orden de la sección 8 (4) permitía la adquisición de grandes volúmenes de comunicaciones, las personas autorizadas dentro de la agencia interceptora podían aplicar selectores fuertes y consultas complejas para generar un índice (ver párrafo 96 anterior). Este proceso de selección estaba circunscrito por la sección 16 (2) de la RIPA y el párrafo 7.19 del Código IC, que disponía que un selector no podía referirse a una persona que se sabía que se encontraba en las Islas Británicas, ni tener como finalidad la identificación del material contenido en las comunicaciones enviadas por o destinadas a él o ella, a menos que el Secretario de Estado hubiera autorizado el uso del selector, habiendo considerado primero que era necesario en interés de la seguridad nacional, con el fin de prevenir o detectar delitos graves, o con el fin de salvaguardar el bienestar económico del Reino Unido en la medida en que esos intereses también fueran relevantes para los intereses de la seguridad nacional; y fuera proporcionado (ver párrafos 85 y 96 anteriores).

385. Un analista solo podía visualizar el material previsto en el índice (véanse los párrafos 96 y 289 anteriores); y no estaba permitido realizar ningún informe de inteligencia de cualquier comunicación o datos relacionados con las comunicaciones a menos que hubieran sido visualizadas por un analista (véase el párrafo 289 anterior). Además, el párrafo 7.13 del Código IC disponía que solo el material descrito en el certificado de la Secretaría de Estado estaba disponible para el examen humano, y a ningún funcionario le estaba permitido obtener acceso al material de otra manera que no fuera la establecida por el certificado (véase el párrafo 96 anterior). El párrafo 6.4 disponía además que antes de que se pudiera acceder a una comunicación en particular por una persona autorizada perteneciente a la agencia interceptora, dicha persona tenía que explicar por qué era necesario el acceso sobre la base de alguna de las razones establecidas en el certificado adjunto, y por qué era proporcionado dadas las circunstancias particulares, teniendo en cuenta si la información podía haber sido obtenida razonablemente por medios menos intrusivos (véase el párrafo 96 anterior).

386. El certificado del Secretario de Estado se expedía cuando concedía la orden y tenía por finalidad garantizar que se aplicara un proceso de selección al material interceptado de modo que solo el material descrito en el certificado se pusiera a disposición para su examen humano (véanse los apartados 6.3y 6.14 del Código IC en el párrafo 96 anterior). Aunque el certificado desempeñó un papel importante en la regulación del acceso al material interceptado, los informes del ISC y del Revisor Independiente de Legislación Terrorista criticaron el hecho de que el material identificado en estos certificados estaba redactado en términos muy generales (por ejemplo, “material que proporciona inteligencia sobre terrorismo tal como se define en la Ley de Terrorismo de 2000 (conforme fue modificada)”) (ver párrafo 342 de la sentencia de la Sala y párrafos 146 y 155 anteriores). El Tribunal coincide con la Sala en que esto suponía una deficiencia del sistema de salvaguardas del régimen de la sección 8 (4).

387. No obstante, según el ISC, aunque el certificado establecía las categorías generales de información que podían examinarse, en la práctica era la selección de los portadores, la aplicación de selectores simples y criterios de búsqueda inicial, y luego de las búsquedas complejas las que determinaban qué comunicaciones se examinaban (véanse los párrafos 146 a 147 anteriores). En otras palabras, mientras que los certificados regulaban la selección del analista del material a partir de un índice generado por ordenador, era la elección de los portadores y selectores / términos de búsqueda los que determinaban qué comunicaciones estaban en ese índice (y por lo tanto eran elegibles

para examen) en primer lugar. Sin embargo, el Tribunal ya ha sostenido que tanto la falta de identificación de las categorías de selectores en la solicitud de la orden como la ausencia de previa autorización interna de aquellos selectores fuertes vinculados a un individuo representaban deficiencias del régimen de la sección 8 (4) (ver párrafo 382 anterior). Estas deficiencias habían sido exacerbadas por la naturaleza genérica del certificado del Secretario de Estado. No solo no había autorización previa e independiente de las categorías de selectores utilizados para generar el índice, ni autorización interna de esos selectores fuertes vinculados a una persona identificable, sino que el certificado que regula el acceso al material de ese índice se redactó en términos insuficientemente precisos para proporcionar cualquier restricción significativa.

388. El párrafo 7.16 del Código IC requería además que el analista que solicitara el acceso al material del índice indicara cualquier circunstancia que pudiera dar lugar a un grado de intrusión colateral de la privacidad, junto con las medidas adoptadas para reducir el alcance de esa intrusión (véase el párrafo 96 anterior). Cualquier acceso posterior por parte del analista se limitaba a un período de tiempo definido, y si ese período de tiempo se renovaba, el registro tenía que ser actualizado proporcionando las razones para tal renovación (ver párrafo 7.17 del Código IC, en párrafo 96 anterior). De acuerdo con el párrafo 7.18 del Código IC, se llevarían a cabo auditorías que incluyeran las oportunas verificaciones para asegurar que los registros solicitando acceso al material eran compilados correctamente, y que el material solicitado estaba dentro de las materias previstas en el certificado del Secretario de Estado (ver párrafo 96 anterior).

389. Además, de acuerdo con el párrafo 7.15, el material recopilado bajo una orden de las previstas en la sección 8(4) solo podía ser leído, visualizado o escuchado por las personas autorizadas (analistas) que habían recibido una formación periódica obligatoria con respecto a las disposiciones de la RIPA y los requisitos de necesidad y proporcionalidad, y quienes habían sido oportunamente evaluados (ver párrafo 96 sobre). De conformidad con el párrafo 7.10, la evaluación de cada miembro del personal se revisaba periódicamente (véase el párrafo 96 anterior).

390. El párrafo 7.6 del Código IC disponía que el material interceptado podía copiarse únicamente en la medida en la que fuera necesario para los fines autorizados y con sujeción a una aplicación estricta del principio de “necesidad de saber”, incluyendo meros extractos o resúmenes cuando esto fuera suficiente para satisfacer la necesidad de conocimiento del usuario. La sección 15(5) de la RIPA requería la existencia de disposiciones para asegurar que cada copia del material o de los datos que se hiciera era almacenada, durante el tiempo que estaban retenidos, de manera segura (ver párrafo 81 anterior); y el párrafo 7.7 requería, además, que antes de su destrucción, el material interceptado, y todas las copias, extractos y resúmenes del mismo, fueran almacenados de forma segura y que no pudieran ser accesibles a personas sin el preceptivo nivel de autorización de seguridad (véase el párrafo 96 anterior).

391. Sin perjuicio de las deficiencias antes mencionadas relativas a la autorización de los selectores (véanse los párrafos 381 y 382 anteriores) y el carácter genérico del certificado del Secretario de Estado (véase el párrafo 386 anterior), el Tribunal considera que las circunstancias en las que el material interceptado podía ser seleccionado, examinado, utilizado y almacenado bajo el régimen la sección 8 (4) eran

suficientemente "previsibles" a los efectos del artículo 8 del Convenio, y que proporcionaban las salvaguardas adecuadas frente a los abusos.

- *5. Las precauciones a adoptar en las comunicaciones del material interceptado a terceras partes.*

392. La sección 15 (2) de la RIPA requería que las siguientes cuestiones se limitaran al mínimo necesario para los "fines autorizados": el número de personas a quién se divulgaba o ponía a disposición el material o los datos; la medida en qué dicho material o los datos se divulgaban o se ponían a disposición; la medida en qué el material o los datos se copiaban; y el número de copias que eran realizadas (véanse el párrafo 78 anterior). De conformidad con la sección 15 (4) y el párrafo 7.2 del Código IC, era necesario para los fines autorizados si, y sólo si continuaba siendo, o era probable que fuera necesario para los fines mencionados en la sección 5 (3) de la RIPA; para facilitar la realización de cualquiera de las funciones de interceptación del Secretario de Estado; para facilitar el desempeño de cualquier función del Comisionado IC o del IPT; para asegurarse de que una persona que lleva a cabo un proceso penal tenga la información necesaria para determinar lo que le requiera el deber de asegurar la imparcialidad de la acusación (aunque el material de interceptación no podía utilizarse en el enjuiciamiento de un delito (véase el párrafo 8.3 de la Código IC en el párrafo 96 anterior); o para el desempeño de cualquier deber impuesto a cualquier persona en virtud de la legislación sobre registros públicos (véanse los párrafos 80 y 96 anteriores).

393. El párrafo 7.3 del Código IC prohibía la divulgación a personas que no habían sido evaluadas adecuadamente y también con base al principio de "necesidad de saber": el material interceptado no podía ser revelado a ninguna persona a menos que las obligaciones de dicha persona, que tenían que estar relacionadas con uno de los fines autorizados, fueran tales que él o ella "necesitara conocer" el material interceptado para desempeñar tales obligaciones o deberes. De la misma manera, solo una parte del material interceptado podía divulgarse como el destinatario necesario (véase el párrafo 96 anterior). El párrafo 7.3 se aplicaba igualmente a la divulgación a personas adicionales dentro de una agencia, y a la divulgación fuera de la agencia (véase el párrafo 96 anterior). De conformidad con el párrafo 7.4, también se aplicaba no solo al interceptor original, sino también a cualquier persona a quien se haya enviado posteriormente el material interceptado (véase el párrafo 96 anterior).

394. Como observó la Sala, dado que la expresión "probablemente sea necesario" no se definía con detalle en la RIPA ni en el Código IC, ni en ningún otro lugar, la sección 15 (4) y el párrafo 7.2 podían, en la práctica, haber dado a las autoridades un amplio poder para revelar y copiar el material interceptado. Sin embargo, el material solo podía ser revelado a una persona con el nivel apropiado de habilitación de seguridad, que tuviera una "necesidad de conocer", y sólo la parte del material interceptado que el individuo necesitaba saber podía ser revelada. Por lo tanto, el Tribunal coincide con la Sala en que la inclusión de la expresión "probablemente sea necesario" no reduce significativamente las salvaguardas para la protección de los datos obtenidos mediante interceptación masiva (véanse los párrafos 368 y 369 de la sentencia de Sala).

395. Pasando, entonces, a la transferencia de material interceptado fuera del Reino Unido, cuando el material había sido interceptado de acuerdo con el derecho interno, el Tribunal considera que el traslado de ese material a un socio de inteligencia extranjero o

a una organización internacional solo implicaría la vulneración del artículo 8 del Convenio si el Estado interceptor no se aseguraba primero de que su socio de inteligencia, en el manejo del material, tuviera en vigor salvaguardas capaces de prevenir los abusos y las interferencia desproporcionadas, y en particular, de que pudiera garantizar el almacenamiento seguro del material y restringir su posterior divulgación (véase el párrafo 362 anterior).

396. En el Reino Unido parecía que los socios de los Cinco Ojos podían acceder a productos resultantes de las órdenes de interceptación de la GCHQ en sus propios sistemas (véase el apartado 180 anterior). En tales casos, la intercepción del material por los servicios de inteligencia del Reino Unido se había llevado a cabo de conformidad con la legislación interna, incluida, en la medida en que resulta aplicable al presente caso, la sección 8(4) de la RIPA. De acuerdo con el párrafo 7.5 del Código IC, cuando el material interceptado era revelado a las autoridades de un país o territorio fuera del Reino Unido, los servicios de inteligencia tenían que tomar medidas razonables para asegurarse que las autoridades en cuestión tenían y mantendrían los procedimientos necesarios para salvaguardar el material interceptado y garantizar que se divulgara, copiara, distribuyera y retuviera sólo en la medida mínima necesaria. El material interceptado no podía ser divulgado a las autoridades de un tercer país o territorio a menos que se acordara explícitamente con la agencia emisora y tenía que ser devuelto a la agencia emisora o destruido de forma segura cuando ya no fuera necesario (véase el párrafo 96 anterior). La Sección 15(7) de la RIPA además disponía que las restricciones que debían estar en vigor debían impedir la realización de cualquier acción relacionada con procedimientos legales fuera del Reino Unido que divulgara el contenido o los datos relacionados con las comunicaciones de una comunicación interceptada cuando tal divulgación no podía haberse realizado en el Reino Unido (véase el párrafo 82 anterior).

397. Con respecto al material confidencial, el párrafo 4.30 del Código IC establecía que cuando la información confidencial se difundiera a un organismo, se tenían que tomar medidas razonables para marcar la información como confidencial. Cuando hubiera alguna duda sobre la legalidad de la diseminación de información confidencial propuesta, se tenía que buscar el consejo de un asesor legal dentro de la agencia interceptora y antes de que pudiera tener lugar una mayor difusión del material (véase el párrafo 96 anterior).

398. Por lo tanto, existían salvaguardas para asegurar que los socios de inteligencia garantizaran el almacenamiento seguro del material transferido y restringieran su posterior divulgación. Una última salvaguarda, a la que el Tribunal concede un peso particular, es la supervisión realizada por el Comisionado IC y el IPT (véanse los párrafos 411 y 414 siguientes).

399. A la luz de lo anterior, el Tribunal considera que las precauciones tomadas al comunicar el material interceptado a otras partes fueron suficientemente claras y con garantías suficientemente sólidas frente a los abusos.

> *- 6. Los límites relativos a la duración de la interceptación, el almacenamiento del material interceptado y las circunstancias en las que dicho material debía ser borrado o destruido.*

400. En cuanto a la duración de las órdenes emitidas conforme a la sección 8 (4) por razones de seguridad nacional o del bienestar económico del Reino Unido, en la medida

en que esos intereses también fueran relevantes para los intereses de la seguridad nacional, de conformidad con la sección 9 de la RIPA, dejaban de tener efecto tras seis meses, a menos que fueran renovadas. Las órdenes de la sección 8 (4) emitidas por el Secretario de Estado a los efectos de prevenir delitos graves dejaban de tener efecto tras tres meses, a menos que se renovaran. Estas órdenes eran renovables por períodos de seis y tres meses, respectivamente, y podían renovarse en cualquier momento antes de su fecha de caducidad mediante una solicitud a la Secretaría de Estado. Esa solicitud tenía que contener la misma información que la solicitud original, junto con una evaluación del valor de la interceptación hasta ese momento y una explicación de por qué era necesario continuar con la misma, en el sentido previsto en la sección 5 (3), y ser proporcionada (ver sección 9 de la RIPA en el párrafo 67 anterior y los párrafos 6.22-6.24 del Código IC en el párrafo 96 anterior). El Secretario de Estado debía cancelar una orden -incluso antes de su vencimiento - si consideraba que ya no era necesaria para los fines previstos en la sección 5 (3) (ver sección 9 de la RIPA en el párrafo 67 anterior).

401. En vista de la clara limitación de la duración de las órdenes de la sección 8 (4), y el requisito de que se mantuvieran bajo revisión continua, el Tribunal considera que las normas relativas a la duración de la interceptación bajo el régimen de la sección 8 (4) eran lo suficientemente claras y proporcionaban salvaguardas frente al abuso.

402. El párrafo 7.9 del Código IC disponía que cuando el servicio recibía material interceptado sin analizar y datos relacionados con las comunicaciones bajo una orden de la sección 8(4), tenía que especificar los períodos máximos de retención para las diferentes categorías de material que reflejaran su naturaleza y grado de intrusión. Esos períodos especificados normalmente no eran de más de dos años, y tenían que ser acordados con el Comisionado IC. En la medida de lo posible, todos los períodos de retención tenían que ser implementados mediante un proceso de eliminación automática, activado una vez que se había alcanzado el período máximo de conservación aplicable (véase el párrafo 96 anterior). De conformidad con el párrafo 7.8 del Código IC, el material interceptado retenido tenía que ser revisado en intervalos de tiempo apropiados para confirmar que la justificación para su retención seguía siendo válida bajo la sección 15(3) de la RIPA (ver párrafo 96 anterior).

403. En sus alegaciones ante la Gran Sala, el Gobierno proporcionó más información sobre los períodos de retención. Las comunicaciones a las que solo se les aplicaba el proceso de “selector fuerte” eran descartadas inmediatamente a menos que coincidieran con el selector fuerte. Las comunicaciones a las que se les aplicaba el proceso de “consulta compleja” se mantenían durante unos días, con el fin de permitir la ejecución del proceso, y luego eran eliminadas automáticamente a menos que hubieran sido seleccionadas para su examen. Las comunicaciones que habían sido seleccionadas para su examen podían conservarse sólo cuando fuera necesario y proporcionado hacerlo. La postura por defecto era que el período de retención para las comunicaciones seleccionadas no era de más de unos pocos meses, después de los cuales se eliminaban automáticamente (aunque si el material había sido citado en informes de inteligencia el informe se mantenía), pero en circunstancias excepcionales se podían retener las comunicaciones seleccionadas durante un periodo de tiempo superior (véase el párrafo 293 anterior). En la práctica, por lo tanto, parecía que los períodos de retención eran significativamente menores que el período máximo de retención de dos años.

404. Finalmente, la sección 15 (3) de la RIPA y el párrafo 7.8 del Código IC requerían que cada copia del material interceptado (junto con los extractos y resúmenes) se destruyera de forma segura tan pronto como la conservación del mismo dejara de ser necesaria para cualquiera de los fines previstos en la sección 5 (3) (véanse los párrafos 79 y 96 anteriores).

405. En el procedimiento *Liberty*, el IPT consideró que las disposiciones sobre la retención de material y su destrucción eran adecuadas (ver párrafo 50 anterior). El Tribunal también considera que las disposiciones "por debajo de la línea de flotación" que establecen las circunstancias en las que el material interceptado debe ser borrado o destruido eran lo suficientemente claras. Sin embargo, en su opinión, hubiera sido deseable que los períodos de retención más cortos identificados por el Gobierno en el curso del presente procedimiento se hubieran reflejado en la legislación pertinente y / o en otras medidas en general.

- 7. Supervisión

406. La supervisión del régimen de la sección 8 (4) estuvo a cargo principalmente del Comisionado IC, aunque según dicho Comisionado "la función esencial de aseguramiento de la calidad [era] realizada inicialmente por el personal y abogados de la agencia de interceptación o el departamento de otorgamiento de órdenes", que brindaban un asesoramiento independiente al Secretario de Estado y realizaban un importante escrutinio previo a la autorización de solicitudes de órdenes y renovaciones para asegurarse de que fueran (y siguieran siendo) necesarias y proporcionadas (véase párrafo 170 anterior).

407. El Comisionado IC era independiente del ejecutivo y del legislativo, y tenía que haber ocupado un alto cargo judicial. Su principal deber era revisar el ejercicio y desempeño, por las Secretarías de Estado correspondientes y las autoridades públicas, de los poderes previstos en la Parte 1 (y en una medida limitada en la Parte 3) de la RIPA y supervisó el régimen de inspección y supervisión que le permitió llevar a cabo una supervisión independiente de cómo se aplicó la ley. Informaba sobre sus actividades, semestralmente, al Primer Ministro, y preparaba un informe anual que se presentaba ante ambas Cámaras del Parlamento. Además, después de cada inspección se enviaba un informe al alto cargo de la agencia inspeccionada que contenía recomendaciones formales y en el que se requería a la agencia para que informara en el plazo de dos meses sobre si se habían implementado las recomendaciones o qué progreso se había realizado. Sus informes periódicos se han publicado desde 2002, y desde 2013 se publican íntegramente salvo los anexos confidenciales. Además, la sección 58 (1) de la RIPA imponía la obligación legal a todos los funcionarios públicos de una organización que se encontrara dentro del mandato del Comisionado IC de facilitarle o proporcionarle todos los documentos o la información que pudiera ser necesaria para permitirle el desempeño sus funciones (véanse los párrafos 135 y 136 anteriores).

408. El informe del Comisionado IC de 2016 proporciona evidencias del alcance de sus facultades de control. En resumen, durante las inspecciones se evaluaban los sistemas establecidos para la interceptación de las comunicaciones y se aseguraba de que se hubieran mantenido todos los registros pertinentes; se examinaban las solicitudes de interceptación seleccionadas para evaluar si cumplían con los requisitos de necesidad y

la proporcionalidad; se entrevistó a oficiales y analistas para evaluar si las interceptaciones y las justificaciones para adquirir todo el material fueron proporcionadas; se examinaban las aprobaciones orales urgentes para verificar que el proceso fue justificado y utilizado apropiadamente; se revisaban aquellos casos en los que comunicaciones sujetas a privilegio legal o u otro tipo de información confidencial había sido interceptada y retenida, y cualquier caso en el que un abogado fuera objeto de una investigación; se revisaba la idoneidad de las salvaguardas y disposiciones adoptadas bajo las secciones 15 y 16 de la RIPA; se investigaba los procedimientos establecidos para la retención, almacenamiento y destrucción del material interceptado y datos relacionados con las comunicaciones; y se revisaban los errores informados y la suficiencia de las medidas implementadas para prevenir su recurrencia (ver párrafo 171 anterior).

409. Durante 2016, la oficina del Comisionado IC inspeccionó a las nueve agencias de interceptación una vez y a los cuatro principales departamentos que otorgaban las órdenes dos veces. Novecientas setenta órdenes fueron inspeccionadas, representando el sesenta y un por ciento del número de órdenes vigentes al cierre del ejercicio y el treinta y dos por ciento del total de nuevas órdenes emitidas en 2016 (ver párrafos 173 y 175 anteriores).

410. Las inspecciones generalmente involucran un proceso de tres etapas. Primero, para lograr una muestra representativa de las órdenes, los inspectores las seleccionaban en base a diferentes tipos de delitos y amenazas a la seguridad nacional, centrándose en los de particular interés o sensibilidad. En segundo lugar, los inspectores examinaban en detalle las órdenes seleccionadas y la documentación asociada durante los días de lectura que precedían a las inspecciones. En esta etapa, los inspectores examinaban las declaraciones de necesidad y proporcionalidad elaboradas por los analistas al agregar un selector al sistema de interceptación para su examen. Cada declaración tenía que valerse por sí misma y tenía que referirse al requisito general de prioridades para la recopilación de inteligencia. En tercer lugar, identificaban aquellas órdenes, operaciones o áreas del proceso que requerían mayor información o aclaración y se disponían a entrevistar al personal operativo, legal o técnico pertinente. Cuando era necesario, examinaban más documentación o sistemas relacionados con esas órdenes (véase el párrafo 174 anterior).

411. El Comisionado IC también supervisaba el intercambio de material interceptado con los socios de inteligencia. En su informe de 2016 indicó que la GCHQ había proporcionado a sus inspectores “detalles completos de los acuerdos de intercambio mediante los cuales los socios de los Cinco Ojos pueden acceder a elementos producto de las órdenes de interceptación de la GCHQ en sus propios sistemas”. Además, sus inspectores pudieron reunirse con representantes de los Cinco Ojos y recibieron una demostración de cómo el resto de miembros de los Cinco Ojos podían solicitar acceso al material interceptado por la GCHQ. Se observó que “el acceso a los sistemas de la GCHQ estaba estrictamente controlado y tenía que justificarse de acuerdo con las leyes del país anfitrión y las instrucciones de manejo de las salvaguardas de las secciones 15/16.” Observó además que antes de recibir cualquier acceso al material interceptado por la GCHQ, los analistas de los Cinco Ojos tenían que completar el mismo proceso de capacitación legal que el personal de la GCHQ (ver párrafo 180 anterior).

412. A la luz de lo anterior, el Tribunal considera que el Comisionado IC proporcionó una supervisión independiente y efectiva del régimen de la sección 8(4). En particular,

él y sus inspectores fueron capaces de evaluar la necesidad y la proporcionalidad de un número significativo de solicitudes de órdenes y la posterior elección de selectores, y de investigar los procedimientos establecidos para la conservación, almacenamiento y destrucción de comunicaciones interceptadas y datos relacionados con las comunicaciones. Ellos tenían también la capacidad de realizar recomendaciones formales a los altos cargos de las autoridades públicas competentes y dichas autoridades estaban obligadas a informar, dentro del plazo de dos meses, sobre el progreso que habían hecho en la implementación de esas recomendaciones. Además, el Gobierno confirmó en sus alegaciones ante la Gran Sala que el Comisionado IC también era informado regularmente por la GCHQ de la base sobre la cual se seleccionaban los portadores para la interceptación (véanse los párrafos 136 y 290 anteriores). Los servicios de inteligencia estaban obligados a mantener registros en cada etapa del proceso de interceptación masiva y estaban obligados a dar acceso a los inspectores a esos registros (véanse los párrafos 6.27 y 6.28 del Código IC en el párrafo 96 anterior). Finalmente, también habían supervisado el intercambio del material interceptado con los socios de inteligencia (véase el párrafo 180 anterior).

– 8. Revisión ex post facto.

413. La revisión *ex post facto* fue realizada por el IPT que en el presente el caso fue presidido en todo momento por un juez del Tribunal Superior. La Sala concluyó - y los demandantes no lo han negado- que el IPT proporcionó un recurso efectivo para los demandantes en cuanto a sus reclamaciones sobre ambas incidencias: la vigilancia y el cumplimiento general del Convenio por los regímenes de vigilancia (ver párrafo 265 de la sentencia de la Sala). Al respecto, la Sala consideró significativo que el IPT tuviera una amplia jurisdicción para examinar cualquier reclamación de interceptación ilegal la cual no dependía de la notificación de la interceptación al sujeto (ver párrafo 122 anterior). En consecuencia, cualquier persona que creyera que había estado sujeto/a a vigilancia secreta podía presentar una demanda. Sus miembros debían haber ocupado un alto cargo judicial o ser abogados cualificados con al menos diez años de experiencia profesional (véase el párrafo 123 anterior). Aquellas personas involucradas en la autorización y ejecución de una orden de intercepción fueron requeridas para revelarles todos los documentos que pudieran necesitar, incluidos los documentos “por debajo de la línea de flotación” que no pudieron hacerse públicos por razones de seguridad nacional (véase el párrafo 125 anterior). Además, tenía la facultad discrecional de celebrar vistas, públicas cuando fuera posible (véase el párrafo 129 anterior); en los procedimientos a puerta cerrada, podían solicitar al abogado del Tribunal que presentara alegaciones en nombre de los demandantes que no pudieron estar representados (véase el párrafo 132 anterior); y cuando resolvía una reclamación tenía la facultad de conceder una compensación y realizar cualquier otra petición que considerara oportuna, incluida la anulación o cancelación de cualquier orden y exigir la destrucción de cualquier registro (ver párrafo 126 anterior). Finalmente, sus fallos legales eran publicados en su propio sitio web, mejorando así el nivel de escrutinio concedido a las actividades de vigilancia en el Reino Unido (ver *Kennedy*, citada anteriormente, § 167).

414. Además, el IPT tenía jurisdicción para conocer sobre cualquier reclamación relativa al cumplimiento del Convenio ya fuera de la transferencia de material interceptado a terceros, o sobre el régimen que regía la transferencia del material interceptado. En el caso de autos, sin embargo, los demandantes del tercero de los asuntos acumulados no formularon ninguna reclamación específica al respecto en el

curso del proceso interno. Más bien, sus reclamaciones sobre el intercambio de inteligencia se centraban únicamente en el régimen que regula la recepción de inteligencia de terceros países (véanse los apartados 467 a 512 siguientes).

415. Por lo tanto, el Tribunal considera que el IPT proporcionaba un sólido recurso judicial a cualquier persona que sospechara que sus comunicaciones habían sido interceptadas por los servicios de inteligencia.

(3) Los datos relacionados con las comunicaciones.

416. El Tribunal ha señalado que en el contexto de la interceptación masiva la interceptación, retención y búsqueda de datos relacionados con las comunicaciones debían analizarse con referencia a las mismas salvaguardas aplicables al contenido, pero que las disposiciones legales que rigen el tratamiento de los datos relacionados con las comunicaciones no tienen que ser necesariamente idénticas en todos los aspectos a las que rigen el tratamiento del contenido (véanse los párrafos 363-364 anteriores). Las órdenes de la sección 8(4) del Reino Unido autorizaban la interceptación de ambos contenido y datos relacionados con las comunicaciones. Estos últimos eran, en la mayoría de los aspectos, tratados de manera idéntica bajo el régimen de la sección 8(4). Así, las deficiencias ya identificadas con respecto al régimen que rige la interceptación del contenido (véanse los párrafos 377, 381 y 382 anteriores) aplican igualmente a los datos relacionados con las comunicaciones, a saber: la ausencia de autorización independiente (ver párrafo 377 anterior); la falta de identificación de las categorías de selectores en la solicitud de la orden (véanse los párrafos 381 y 382 anteriores); la falta de sometimiento de los selectores vinculados a personas físicas identificables a autorización interna; y la falta de previsibilidad de las circunstancias en qué las comunicaciones podían ser examinadas (véase el párrafo 391 anterior), teniendo en cuenta tanto la falta de identificación de las categorías de selectores en la solicitud de la orden (véanse los párrafos 381 y 382 anteriores) y la naturaleza genérica del certificado del Secretario de Estado (ver párrafo 386 anterior).

417. Al mismo tiempo, el tratamiento de los datos relacionados con las comunicaciones se benefició en su mayor parte de las mismas garantías que se aplicaban al contenido. Como este último, los primeros estaban sujetos a un proceso de filtrado automatizado casi en tiempo real, en el que una proporción sustancial de ellos eran eliminados instantáneamente en esta etapa; y también eran objeto de consultas simples o complejas con el fin de extraer el material que era de potencial valor de inteligencia. Además, los selectores utilizados con respecto a los datos relacionados con las comunicaciones estaban sujetos a las mismas salvaguardas que los del contenido; en particular, los analistas tenían que completar un registro escrito que explicara por qué era necesario cada nuevo selector agregado al sistema y proporcionado, ese registro estaba sujeto a auditoría por parte del Comisionado IC, los selectores tenían que ser eliminados si se establecía que no estaban siendo utilizados para el objetivo previsto, y había un tiempo máximo durante el cual los selectores podían permanecer en uso antes de que fuera necesaria una revisión (ver párrafo 298 anterior).

418. El contenido y los datos relacionados con las comunicaciones también estaban sujetos a muchos de los mismos procedimientos de almacenamiento, acceso, examen y uso, a las mismas precauciones para su comunicación a terceros, y a los mismos procedimientos de borrado y destrucción. En este sentido, tanto el contenido como los

datos relacionados con las comunicaciones estaban sujetos a las salvaguardas de la sección 15 de la RIPA; los analistas que deseaban acceder a datos relacionados con las comunicaciones tenían que completar un registro auditable en el que se explicara por qué era necesario el acceso y proporcionado; y no se podían realizar informes de inteligencia sobre la base de datos relacionados con las comunicaciones a menos que y hasta que hubieran sido examinados.

419. Sin embargo, había dos cuestiones principales en las que el régimen de interceptación trataba al contenido y a los datos relacionados con las comunicaciones de forma diferente: los datos relacionados con las comunicaciones se excluyeron de la salvaguarda de la sección 16 (2), lo que significaba que si un analista deseaba utilizar un selector referible a un individuo que se conocía que se encontraba en ese el momento en las Islas Británicas, no estaba obligado/a a tener certificado el uso de ese selector como necesario y proporcionado por el Secretario de Estado; y los datos relacionados con comunicaciones que no coincidían ni con un selector fuerte ni con consultas complejas no se destruían inmediatamente, sino que se almacenaban por un período máximo de hasta varios meses (véanse los párrafos 296 a 298 anteriores). Por lo tanto, el Tribunal examinará si el derecho interno definió claramente los procedimientos a seguir para seleccionar datos relacionados con las comunicaciones para su examen, y los límites sobre la duración del almacenamiento de estos datos.

420. En el marco del régimen de la sección 8(4), la sección 16(2) era la principal salvaguarda legal que circunscribía el proceso de selección del material interceptado para su examen. Sin embargo, no era la única salvaguarda. Como ya se ha mencionado en el párrafo 417 anterior, todos los nuevos selectores tenían que ser justificados por los analistas a través de la creación de un registro escrito en el que se explicara por qué la elección del selector era necesaria y proporcionada (ver párrafos 291 a 292 y 298 anteriores); los analistas que desearan examinar los datos relacionados con las comunicaciones tenían que completar un registro adicional explicando por qué era necesario y proporcionado hacerlo, en cumplimiento de las normas sobre las funciones legales de la GCHQ (véase el párrafo 6.4 del Código IC, en el párrafo 96 anterior); y estos registros eran objeto de auditoría y supervisión por parte del Comisionado IC (véanse los párrafos 135 a 136 y 381 anteriores). Según el Gobierno, no hubiera sido factible extender la salvaguarda de la sección 16 (2) a los datos relacionados con las comunicaciones, ya que esto habría requerido que el Secretario del Estado certificara la necesidad y proporcionalidad de focalizarse en el individuo afectado en cada caso. El número de consultas realizadas sobre los datos de las comunicaciones fueron significativamente más elevadas que el número de consultas realizadas sobre el contenido (posiblemente muchos miles en una semana determinada en relación con personas que se sabía o se creía que se encontraban en el Reino Unido), y en muchos de estos casos no se conocería la identidad del individuo. Además, el Gobierno señaló que los datos relacionados con las comunicaciones tenían un carácter temporal, y tener que retrasar la realización de búsquedas haciéndolas depender de la adquisición de una autorización individual implicaría un grave riesgo de socavar su uso en términos de inteligencia (véase el párrafo 296 anterior).

421. El Tribunal acepta que los datos relacionados con las comunicaciones son una herramienta esencial para los servicios de inteligencia en la lucha contra el terrorismo y los delitos graves, y que había circunstancias en las que era necesario y proporcionado buscar y acceder a los datos relacionados con las comunicaciones de personas que se

conocía que se encontraban en el Reino Unido. Además, mientras la sección 16 (2) contiene una importante salvaguarda que rige el proceso de selección del material interceptado para su examen, es digno de mención que al evaluar el régimen que rige la interceptación masiva del contenido, el Tribunal dio mucho más peso a la existencia o no de un mecanismo eficaz para garantizar que la elección de los selectores estuviera sujeta a los requisitos de necesidad y proporcionalidad del Convenio; y sujeta tanto a la supervisión interna como externa. Por lo tanto, si bien el Tribunal se hace eco de las preocupaciones planteadas con respecto a la elección y supervisión de los selectores en los párrafos 381 y 382 anteriores, no considera que la exclusión de los datos relacionados con las comunicaciones de la salvaguarda de la sección 16 (2) deba aportar un peso decisivo en la valoración global.

422. En cuanto a la duración del almacenamiento, el Gobierno sostuvo que los datos relacionados con las comunicaciones "requieren de un mayor trabajo analítico, durante un periodo más largo, para descubrir 'incógnitas desconocidas'". Ese descubrimiento podía implicar un ejercicio de juntar pequeños elementos dispares de datos relacionados con las comunicaciones para formar un "rompecabezas" que revelara una amenaza, e incluía el posible examen de elementos que inicialmente parecían no ser de interés para la inteligencia. Descartar los datos de las comunicaciones no seleccionados inmediatamente, o incluso después de unos pocos días, haría imposible ese ejercicio (véase el párrafo 297 anterior).

423. En vista de lo anterior, y en vista de que existió un plazo máximo de conservación, que no excedía de "varios meses", y de que la diferencia de trato era objetiva y estaba razonablemente justificada, el Tribunal considera que las disposiciones de almacenamiento de los datos relacionados con las comunicaciones eran lo suficientemente sólidas, a pesar de que diferían sustancialmente de las disposiciones relativas al contenido. Sin embargo, estos períodos de conservación sólo fueron revelados en el proceso ante este Tribunal. En consecuencia, los períodos de retención más cortos no eran evidentes para nadie que leyera el Código IC; ni había ninguna indicación en el Código IC de que los períodos de conservación para los datos relacionados con las comunicaciones fueran diferentes de los relativos al contenido. En opinión del Tribunal, para cumplir con el requisito del artículo 8 de "previsibilidad", los períodos de retención revelados en el procedimiento ante él deben incluirse en las medidas legislativas y/u otras medidas generales apropiadas.

(4) Conclusión.

424. El Tribunal acepta que la interceptación masiva es de vital importancia para los Estados contratantes en la identificación de amenazas a su seguridad nacional. Esto ha sido reconocido por la Comisión de Venecia (véase el párrafo 196 anterior) y fue la posición adoptada por el Gobierno demandado, así como por los Gobiernos de Francia y los Países Bajos en sus intervenciones (véanse los párrafos 300 y 303 anteriores). También fue la conclusión del Revisor Independiente de la Legislación de Terrorismo, quien, habiendo examinado una gran cantidad de material cerrado, llegó a la conclusión de que la interceptación masiva era una facultad esencial: primero, porque los terroristas, los criminales y los servicios de inteligencia extranjeros hostiles se habían vuelto cada vez más sofisticados para evadir la detección por los medios tradicionales; y en segundo lugar, porque la naturaleza global de Internet significaba que la ruta por la que una comunicación en particular viajaba se había vuelto enormemente impredecible.

A pesar de que él y su equipo consideraron alternativas a la interceptación masiva (incluyendo la interceptación dirigida, el uso de fuentes humanas y productos comerciales de ciberdefensa), concluyeron que ningunas de dichas alternativas o combinación de alternativas eran suficientes para sustituir el poder de la interceptación masiva (véase el párrafo 166 anterior).

425. No obstante, el Tribunal recuerda que existe un potencial considerable de que se abuse de la interceptación masiva de una manera que afecte negativamente a los derechos de las personas a la vida privada (véase el párrafo 347 anterior). Por tanto, en un Estado de derecho, conforme se menciona expresamente en el Preámbulo del Convenio y es inherente al objeto y al fin del Artículo 8 (ver *Roman Zakharov*, citada anteriormente, § 228), el Tribunal considera que, visto en su conjunto, el régimen de la sección 8 (4), a pesar de sus salvaguardas, incluidas algunas sólidas como se destacó anteriormente (véanse, por ejemplo, los párrafos 412 y 415 anteriores), no contenía suficientes salvaguardas "de extremo a extremo" para brindar garantías adecuadas y efectivas contra la arbitrariedad y el riesgo de abuso. En particular, ha identificado las siguientes deficiencias fundamentales en el régimen: la ausencia de autorización independiente, la falta de inclusión de las categorías de selectores en la solicitud de una orden, y la falta de sujeción de los selectores vinculados a una persona a una autorización interna previa (véanse los párrafos 377 a 382 anteriores). Estas debilidades afectaban no solo a la interceptación del contenido de las comunicaciones, sino también a la interceptación de los datos relacionados con las comunicaciones (véase el párrafo 416 anterior). Si bien el Comisionado IC proporcionó una supervisión independiente y eficaz del régimen, y el IPT ofreció un recurso judicial efectivo para cualquier persona que sospechara que sus comunicaciones habían sido interceptadas por los servicios de inteligencia, estas importantes salvaguardas no eran suficientes para contrarrestar las deficiencias destacadas en los párrafos 377 a 382 anteriores.

426. En vista de las deficiencias antes mencionadas, el Tribunal considera que la sección 8 (4) no cumplía con el requisito de "calidad de la ley" y, por lo tanto, era incapaz de reducir la "interferencia" a lo que fuera "necesario en una sociedad democrática".

427. En consecuencia, se ha producido una violación del artículo 8 del Convenio.

C. La violación del artículo 10 del Convenio alegada.

428. Los demandantes tanto en el segundo como en el tercero de los asuntos acumulados denunciaron la violación del artículo 10 del Convenio por el régimen de la sección 8 (4), argumentando que la protección otorgada por el artículo 10 a las comunicaciones privilegiadas era de vital importancia para ellos como periodistas y ONGs, respectivamente. Sin embargo, como declaró la Sala la reclamación de los demandantes del tercero de los asuntos acumulados era inadmisible por falta de agotamiento de los recursos internos previos, por lo que solo se analizó la denuncia del artículo 10 relativa a los periodistas en el ámbito del caso remitido a la Gran Sala.

429. El artículo 10 del Convenio dispone:

> 1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no

impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa.

2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial.

1. La sentencia de la Sala.

430. La Sala determinó que como las medidas de vigilancia bajo el régimen de la sección 8 (4) no tenían por objeto vigilar a los periodistas o descubrir fuentes periodísticas, la interceptación de tales comunicaciones no podía, por en sí misma, considerarse como una injerencia particularmente grave en la libertad de expresión. Sin embargo, consideró que la interferencia sería mayor si esas comunicaciones eran seleccionadas para su examen. Si ese era el caso, la interferencia sólo podía estar "justificada por un requisito primordial de interés público" si iba acompañada de las salvaguardas suficientes. En particular, las circunstancias en las que se podían seleccionar tales comunicaciones intencionadamente para su examen tenían que establecerse con suficiente claridad en el derecho interno, y tenían que existir medidas adecuadas para garantizar la protección de la confidencialidad cuando tales comunicaciones hubieran sido seleccionadas, intencionadamente o de otro modo, para su examen. En ausencia de disposiciones públicamente accesibles que limitaran las facultades de los servicios de inteligencia para buscar y examinar material periodístico confidencial excepto cuando estaba justificado por un requisito esencial de interés público, la Sala determinó que también se había producido una violación de artículo 10 del Convenio.

2. Alegaciones de las partes.

(a) Los demandantes.

431. Los demandantes en el segundo de los casos acumulados alegaron que el régimen de interceptación masiva infringía el artículo 10 porque la interceptación a gran escala y el mantenimiento de grandes bases de datos de información tenía un efecto escalofriante sobre la libertad de comunicación de los periodistas.

432. En vista de la importancia fundamental de la libertad de prensa, los demandantes sostuvieron que cualquier interferencia en la libertad periodística, y en particular, en el derecho a mantener la confidencialidad de las fuentes empleadas, tenía que ser atendido con garantías procesales legales acordes con la importancia del principio en juego. En particular, la noción "de conformidad con la ley" requería que cuando una medida permitiera identificar fuentes o revelar material periodístico tenía que haber sido autorizada por un juez u otro organismo independiente e imparcial; la revisión tenía que producirse *ex ante*; y el organismo que concedía la autorización debía estar investido de la potestad para determinar si estaba "justificado por un requisito primordial de interés público" y, en particular, si alguna otra medida menos intrusiva podía haber sido suficiente para alcanzar dicho interés público superior (ver *Sanoma Uitgevers B.V. contra los Países Bajos [GC], núm. 38224/03*, 14 de septiembre de 2010). Ninguna de estas salvaguardas estaba presente en el régimen de la sección 8(4).

(b) El Gobierno

433. El Gobierno argumentó, en primer lugar, que no se había establecido en la jurisprudencia del Tribunal la proposición de que se requiriera la previa (o independiente) autorización judicial para el funcionamiento de un régimen de seguimiento estratégico en virtud del cual algún material periodístico podía ser interceptado en el curso del funcionamiento de ese régimen. Más bien, el Tribunal había establecido una fuerte distinción entre el seguimiento estratégico de las comunicaciones y/o datos de comunicaciones, que inesperadamente podían "barrer" algún material periodístico, y las medidas dirigidas al material periodístico (ver *Weber y Saravia*, antes citada, § 151, y contrastar con *Sanoma Uitgevers B.V.*, antes citada, y *Telegraaf Media Nederland Landelijke Media B.V. y otros contra los Países Bajos*, núm. 39315/06, 22 de noviembre de 2012). El requisito de autorización judicial previa no tendría sentido en el contexto de la interceptación masiva, ya que al juez sólo se le podría decir que existía la posibilidad de que la ejecución de la orden pudiera resultar en la interceptación de algún material periodístico confidencial.

434. Dicho esto, el Gobierno aceptó la conclusión de la Sala relativa a que se precisaba de una mayor protección en el momento de la selección para su examen. Por tanto, confirmó que el Código IC se había modificado para estipular que "[p] articular consideración debe darse a la interceptación de comunicaciones o la selección para el examen de contenidos que contengan información cuando las personas puedan haber asumido razonablemente un alto grado de confidencialidad. Esto incluye las comunicaciones que contienen información especialmente protegida por la ley; material periodístico confidencial y las comunicaciones que identifican la fuente de un periodista".

(c) Los terceros intervinientes

(i) El Gobierno de Francia

435. El Gobierno de Francia argumentó que la vigilancia de los periodistas estaba permitida en virtud del artículo 10 del Convenio si con ello se perseguía un objetivo legítimo y era necesaria, y si la medida no tenía como objetivo a periodistas y no tenía como objetivo identificar sus fuentes. Ningún paralelismo podía establecerse entre la situación en la que las comunicaciones de los periodistas eran interceptadas por casualidad, y aquellos casos en los que una decisión de las autoridades nacionales requiriera a un periodista que revelara sus fuentes.

(ii) El Gobierno de Noruega

436. El Gobierno noruego sostuvo que el amplio margen de apreciación permitido en virtud del artículo 8 con respecto a la decisión de introducir un régimen de interceptación masiva también se aplicaba, lógicamente, cuando la decisión era examinada desde el punto de vista del artículo 10. Se derrotaría la naturaleza y el fin de un régimen de interceptación masiva si el Tribunal sometiera la decisión de establecerlo al requisito de "justificado por un requisito primordial de interés público" simplemente porque algunas de las comunicaciones interceptadas pudieran implicar el contacto con periodistas.

(iii) El Relator Especial de las Naciones Unidas sobre la promoción del derecho a libertad de opinión y expresión.

437. El Relator Especial argumentó que las medidas de vigilancia interferían con el derecho a la libertad de expresión y, por lo tanto, tenían que cumplir con el artículo 19 (3) del Pacto Internacional de Derechos Civiles y Políticos, que exigía restricciones sobre la expresión de "sólo las previstas en la ley y que sean necesarias" para la protección de los derechos y la reputación de los demás, la seguridad nacional, el orden público y la salud o moral públicas. Los programas de vigilancia masiva proporcionaban importantes desafíos al requisito de una legislación accesible, debido a la complejidad de cómo funcionaban las tecnologías de vigilancia, los vagos estándares legales para interceptar comunicaciones, y complicados y a menudo clasificados marcos administrativos. Además, hubo una gran preocupación por la proporcionalidad relacionada con la interferencia en el trabajo de los periodistas y la protección de sus fuentes. Como las leyes de derechos humanos preveían un alto nivel de protección de la confidencialidad, las restricciones debían ser excepcionales y aplicadas únicamente por las autoridades judiciales y las evasiones no autorizadas por las autoridades judiciales según normas claras y precisas no se debían utilizar para socavar la confidencialidad de la fuente. En este sentido, el alcance de la protección de las comunicaciones confidenciales tenía que tener en cuenta el concepto amplio de "periodista" bajo el PIDCP.

(iv) Artículo 19

438. Artículo 19 solicitó al Tribunal que concediera la misma protección a las ONGs que a los periodistas.

(v) La Fundación de Helsinki para los Derechos Humanos.

439. La Fundación de Helsinki sostuvo que la protección de las fuentes periodísticas se había visto socavada no solo por la vigilancia del contenido de las comunicaciones de los periodistas, sino también por la vigilancia de los metadatos de las mismas que podían, por sí mismos, permitir la identificación de las fuentes e informantes. Era especialmente problemático que la información confidencial pudiera adquirirse sin el conocimiento de los periodistas o su control, privándolos así de su derecho a invocar la confidencialidad, y de que sus fuentes confiaran en su capacidad de garantizar la confidencialidad.

(vi) Asociación de Abogados de los Medios de Comunicación ("MLA"- siglas en inglés-)

440. La MLA expresó su preocupación por el hecho de que los regímenes de vigilancia masiva permitían interceptar comunicaciones y datos relacionados con las comunicaciones periodísticas que les permitían identificar a las fuentes. En su opinión, la mera interceptación de material periodístico podía interferir con el artículo 10 del Convenio, incluso si el material no era realmente analizado. Por tanto, era imperativo que se establecieran las salvaguardas adecuadas para proteger la confidencialidad de las fuentes periodísticas, independientemente del fin para el cual fuera interceptada la información. Además, un régimen que permite a los Estados interceptar las comunicaciones de periodistas sin autorización judicial previa tenía más probabilidades de afectar al periodismo de interés público porque la naturaleza de tales historias implicaba que el Estado tuviera un interés particular en identificar las fuentes. El riesgo era particularmente grave cuando la fuente fuera un denunciante del Gobierno. El efecto escalofriante del mero potencial de que tales fuentes fueran identificadas era

significativo. Como consecuencia, la MLA argumentó que, al menos, el artículo 10 requería una previa supervisión judicial ante cualquier intento de obtener material periodístico o identificar fuentes periodísticas, y que el proceso judicial debía ser inter partes.

(vii) El Sindicato Nacional de Periodistas ("NUJ" - siglas en inglés-) y la Federación Internacional de periodistas ("FIP"- siglas en inglés-).

441. El NUJ y la FIP sostuvieron que la confidencialidad de las fuentes era indispensable para la libertad de prensa. También expresaron su preocupación por el posible intercambio de datos retenidos por el Reino Unido con otros países. Si se compartiera material periodístico confidencial con un país respecto del que no se podía confiar que lo manejara de forma segura, podía terminar en las manos de personas que pudieran hacer daño al periodista o a su fuente. En opinión de los intervinientes, las salvaguardas del Código IC actualizado y la promulgación del código de prácticas sobre los datos de comunicaciones no eran adecuadas, especialmente cuando el periodista o la identificación de su fuente no era el objetivo de la medida de vigilancia.

3. Evaluación del Tribunal

(a) Principios generales sobre la protección de las fuentes de los periodistas.

442. Dado que la libertad de expresión constituye uno de los fundamentos de una sociedad democrática, el Tribunal siempre ha sometido a las salvaguardas para el respeto de la libertad de expresión en los casos previstos en el artículo 10 del Convenio a un escrutinio especial. Las salvaguardas otorgadas a la prensa son de especial importancia, y la protección de las fuentes periodísticas es una de las piedras angulares de la libertad de prensa. Sin tal protección, las fuentes pueden verse disuadidas de ayudar a la prensa a informar al público sobre asuntos de interés público. Como resultado, el papel vital de vigilancia pública de la prensa puede verse socavado, y la capacidad de la prensa para proporcionar información precisa y de confianza puede verse afectada negativamente (ver, *inter alia*, *Goodwin contra el Reino Unido*, núm. 17488/90, § 39, 27 de marzo de 1996; *Sanoma Uitgevers B.V.*, antes citada, § 50; y *Weber y Saravia*, citada arriba, § 143).

443. Las órdenes de revelar las fuentes pueden tener un impacto perjudicial, no sólo en la fuente, cuya identidad puede ser revelada, sino también en el periódico u otra publicación contra la que se dirige la orden, cuya reputación puede verse afectada negativamente por la divulgación a los ojos de futuras fuentes potenciales; y sobre el público, quienes tienen interés en recibir información obtenida a través de fuentes anónimas. Hay, sin embargo, "una diferencia fundamental" entre las autorizaciones que ordenaban a un periodista revelar la identidad de sus fuentes, y las autorizaciones para realizar registros en la casa y el lugar de trabajo de un periodista con miras a descubrir sus fuentes (comparar con *Goodwin*, citada anteriormente, § 39, con *Roemen y Schmit contra Luxemburgo*, núm. 51772/99, § 57, TEDH 2003-IV). Estas últimas, aunque fueran improductivas, constituyen una medida más drástica que divulgar la identidad de una fuente, ya que los investigadores que allanan el lugar de trabajo del periodista tienen acceso a toda la documentación en poder del mismo (véase *Roemen y Schmit*, antes citada, § 57).

444. Una injerencia en la protección de las fuentes periodísticas no puede ser compatible con el artículo 10 del Convenio a menos que esté justificada por un a requisito primordial de interés público (véase *Sanoma Uitgevers B.V.*, citada anteriormente, § 51; *Goodwin*, citada anteriormente, § 39; *Roemen y Schmit*, citada supra, § 46; y *Voskuil c. los Países Bajos*, núm. 64752/01, párrafo 65, 22 de noviembre de 2007). Además, cualquier injerencia en el derecho a la protección de las fuentes periodísticas debe ir acompañada de procedimientos legales y salvaguardas acordes con la importancia del principio en juego (ver *Sanoma Uitgevers B.V.*, citada anteriormente, §§ 88-89). La primera y más importante de entre estas salvaguardas es la garantía de revisión por un juez u otro organismo independiente e imparcial con el poder de determinar si existe un requisito de interés público que prevalece sobre el principio de protección de las fuentes periodísticas antes de la entrega de dicho material y para evitar el acceso innecesario a información capaz de revelar la identidad de las fuentes si no es así (véase *Sanoma Uitgevers B.V.*, citada anteriormente, §§ 88-90).

445. Dado el carácter preventivo de dicha revisión, el juez u otro organismo independiente e imparcial deben estar en condiciones de sopesar los riesgos potenciales y los respectivos intereses antes de cualquier divulgación y con referencia al material que se pretende divulgar para que los argumentos de las autoridades que solicitan la divulgación puedan ser evaluados adecuadamente. La decisión a tomar debe regirse por criterios claros, incluyendo si una medida menos intrusiva puede ser suficiente para servir a los intereses públicos superiores perseguidos. Debe estar abierta la posibilidad al juez u otro organismo a negarse a emitir una orden de divulgación o a emitir una orden cualificada para proteger las fuentes de ser reveladas, estén o no específicamente nombradas en el material retenido, sobre la base de que la comunicación de dicho material crea un grave riesgo de comprometer la identidad de las fuentes del periodista (ver *Sanoma Uitgevers B.V.*, citada anteriormente, § 92 y *Nordisk Film & TV A/S c. Dinamarca* (dec.), núm. 40485/02, TEDH 2005-XIII). En situaciones de urgencia, debe existir un procedimiento para identificar y aislar, con carácter previo a la explotación del material por parte de las autoridades, la información que podría conducir a la identificación de las fuentes de la información que no conlleve tal riesgo (ver, *mutatis mutandis*, *Wieser y Bicos Beteiligungen GmbH c. Austria*, núm. 74336/01, §§ 62-66, TEDH 2007-XI).

(b) El artículo 10 en el contexto de la interceptación masiva.

446. En el asunto *Weber y Saravia* el Tribunal reconoció que "el régimen de control estratégico" había interferido con la libertad de expresión del primer demandante como periodista. Sin embargo, para ello consideró decisivo que las medidas de vigilancia no estaban dirigidas a monitorear a los periodistas o descubrir fuentes periodísticas. Como tal, consideró que las interferencias con la libertad de expresión del primer demandante no podían caracterizarse como particularmente graves y, en vista de las garantías correspondientes, declaró las reclamaciones inadmisibles por manifiestamente infundadas (véase *Weber y Saravia*, citada anteriormente, §§ 143-145 y 151).

(c) El enfoque que debe adoptarse en el presente caso.

447. Bajo el régimen de la sección 8(4), se podía haber accedido a material periodístico confidencial por los servicios de inteligencia ya sea intencionadamente, a través del uso deliberado de selectores o términos de búsqueda conectados a un periodista o a una

organización de noticias, o involuntariamente, como una "captura incidental" de la operación de interceptación masiva.

448. Cuando la intención de los servicios de inteligencia era acceder a material periodístico confidencial, por ejemplo, mediante el uso deliberado de un selector fuerte conectado a un periodista, o cuando, como resultado de la elección de selectores tan fuertes, existía una alta probabilidad de que dicho material fuera seleccionado para su examen, el Tribunal considera que la injerencia era proporcional a la ocasionada por el registro de la casa de un periodista o de su lugar de trabajo; independientemente de si la intención de los servicios de inteligencia era identificar una fuente, el uso de selectores o términos de búsqueda conectados a un periodista muy probablemente implicaría la adquisición de cantidades significativas de material periodístico confidencial que pueden socavar la protección de las fuentes en un grado aún mayor que una orden de revelar una fuente (ver *Roemen y Schmit*, citada anteriormente, § 57). Por lo tanto, el Tribunal considera que antes de que los servicios de inteligencia utilicen selectores o términos de búsqueda que conocen que están conectados a un periodista, o que hagan la selección de material periodístico confidencial para su examen altamente probable, los selectores o términos de búsqueda deben haber sido autorizados por un juez u otra autoridad independiente u organismo imparcial de toma de decisiones investido con el poder de determinar si estaban "justificados por un requisito primordial de interés público" y, en particular, si una medida menos intrusiva podría ser suficiente para alcanzar el interés público superior que se persigue (ver *Sanoma Uitgevers B.V.*, citada anteriormente, §§ 90-92).

449. Incluso cuando no existe la intención de acceder a la información de material periodístico confidencial, y los selectores y términos de búsqueda utilizados no son tales como para hacer altamente probable la selección de material periodístico confidencial para su examen, no obstante, existirá el riesgo de que dicho material pueda ser interceptado, e incluso examinado, como una "captura incidental" de una operación de interceptación masiva. A juicio del Tribunal, esta situación es materialmente diferente a la vigilancia selectiva de un periodista a través de la sección 8 (1) o los regímenes de la sección 8 (4). Como la interceptación de las comunicaciones de cualquier periodista sería inadvertida, el grado de interferencia de las comunicaciones y / o fuentes periodísticas no se podría predecir desde el principio. En consecuencia, no sería posible en la etapa de autorización para un juez u otro organismo independiente evaluar si tal interferencia estaría "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.

450. En el asunto *Weber y Saravia*, el Tribunal sostuvo que la interferencia con la libertad de expresión provocada por el monitoreo estratégico no podía ser caracterizada como particularmente grave ya que no estaba dirigida a monitorear a los periodistas y las autoridades sólo sabrían al examinar las telecomunicaciones interceptadas, en su caso, si las comunicaciones de un periodista habían sido monitoreadas (ver *Weber y Saravia*, citada arriba, § 151). Por lo tanto, aceptó que la interceptación inicial, sin examen del material interceptado, no constituía una injerencia grave del artículo 10 del Convenio. No obstante, como ya ha señalado el Tribunal, las capacidades tecnológicas de la era actual, cada vez más digital, han aumentado el volumen de las comunicaciones que atraviesan Internet, y, en consecuencia, la vigilancia que no se dirige directamente a las personas tiene la capacidad de tener un alcance muy amplio, tanto dentro como fuera

el territorio del Estado que vigila (véanse los párrafos 322 y 323 anteriores). Como el examen de las comunicaciones de un periodista o de los datos relacionados con las comunicaciones por un analista son capaces de conducir a la identificación de una fuente, el Tribunal considera imperativo que la legislación interna contenga salvaguardas sólidas con respecto al almacenamiento, examen, uso, transmisión posterior y destrucción de dicho material confidencial. Además, incluso si una comunicación periodística o los datos relacionados con una comunicación no han sido seleccionados para el examen a través del uso deliberado de un selector o término de búsqueda que se sabe que está relacionado con un periodista, siempre y cuando se haga evidente que la comunicación o los datos relacionados con la comunicación contienen información confidencial de material periodístico, su almacenamiento continuado y su examen por un analista sólo debería ser posible si lo autoriza un juez u otra autoridad independiente u organismo imparcial de toma de decisiones investido con el poder de determinar si el almacenamiento y examen continuos están "justificados por una requisito primordial de interés público".

(d) Aplicación del citado test a los hechos del presente caso.

451. En el asunto *Weber y Saravia* el Tribunal reconoció expresamente que el régimen de vigilancia impugnado había interferido con el derecho del primer demandante a la libertad de expresión como periodista (ver *Weber y Saravia*, citada supra, §§ 143-145). En el presente caso, el Tribunal ha aceptado que el funcionamiento del régimen de la sección 8(4) interfirió en todos los derechos de los demandantes consagrados en el artículo 8 del Convenio (véanse los párrafos 324 a 331 anteriores). Dado que los demandantes en el segundo de los casos acumulados eran una organización de recopilación de noticias y un periodista, respectivamente, el Tribunal acepta que el régimen de la sección 8(4) también interfiere con sus derechos en virtud del artículo 10 del Convenio a la libertad de expresión como periodistas.

452. Como ya se señaló, el régimen de la sección 8(4) tenía una base clara en el derecho interno (véanse los párrafos 365 y 366 anteriores). Sin embargo, al evaluar la previsibilidad y necesidad en virtud del artículo 8 del Convenio, el Tribunal identificó las siguientes deficiencias en el régimen y sus correspondientes salvaguardas: la ausencia de autorización independiente (ver párrafo 377 anterior); la falta de identificación de las categorías de selectores en la solicitud de una orden (ver párrafos 381-382 anteriores); y la ausencia de autorización interna previa para el uso de selectores vinculados a un individuo identificable (ver párrafo 382 anterior).

453. No obstante, se establecieron algunas salvaguardas adicionales con respecto a la confidencialidad del material periodístico en los párrafos 4.1-4.3 y 4.26-4.31 del Código IC (véase el párrafo 96 anterior). Según el párrafo 4.1, cualquier solicitud de una orden tenía que indicar si era probable que la interceptación diera lugar a una infracción colateral de la privacidad, incluyendo los casos en los que comunicaciones periodísticas estaban involucradas y, cuando era posible, había que especificar las medidas a adoptar para reducir el alcance de la intrusión colateral. Sin embargo, el párrafo 4.1 solo requería que el Secretario de Estado tuviera estas circunstancias y medidas en cuenta al considerar una solicitud para una orden de la sección 8 (1), es decir, una orden que autorizaba una interceptación dirigida. El párrafo 4.2 disponía además que "una consideración especial también debe darse" en los casos en que el material periodístico confidencial pueda estar involucrado, y el párrafo 4.26 establece que "especial

consideración" ha de darse a la interceptación de comunicaciones que involucren material periodístico confidencial.

454. Según el Gobierno, el párrafo 4.28 también se aplicaba al material periodístico confidencial. Cuando la intención era adquirir información personal confidencial, el párrafo 4.28 indicaba que las razones y la necesidad y proporcionalidad específicas para hacerlo tenían que estar claramente documentadas. Si la adquisición de dicho material era probable pero no pretendida, cualquier medida de mitigación posible tenía que ser considerada y, si ninguna estaba disponible, se tenía que considerar si se requerían disposiciones de manipulación especial dentro de la agencia interceptora (ver párrafo 96 anterior). El Tribunal observó, sin embargo, que en el párrafo 4.26 del Código IC, "información personal confidencial" parecía ser un concepto distinto al de "material periodístico confidencial" (véase el párrafo 96 anterior).

455. En cuanto al almacenamiento de material confidencial, el párrafo 4.29 del Código IC disponía que dicho material solo podía conservarse cuando era necesario y proporcionado para uno de los fines autorizados en la sección 15 (4) de la RIPA, y tenía que ser destruido de forma segura cuando ya no se necesitara para uno de esos fines (véase el párrafo 96 anterior). Además, de acuerdo con el párrafo 4.30, si era conservado o difundido a un organismo externo, se tenían que tomar medidas razonables para marcar la información como confidencial. Cuando hubiera alguna duda sobre la legalidad de la diseminación propuesta de la información confidencial, se tenía que solicitar el asesoramiento de un asesor legal de la agencia interceptora pertinente y antes de que pudiera tener lugar una mayor difusión del material (véase el párrafo 96 anterior). Finalmente, el párrafo 4.31 requería que le fuera notificado al Comisionado IC la conservación de dicho material tan pronto como fuera razonablemente posible, y que dicho material se pusiera a su disposición cuando lo solicitara (ver párrafo 96 anterior).

456. A la luz de lo anterior, el Tribunal acepta que las garantías previstas en el Código IC relativas al almacenamiento, transmisión y destrucción del material periodístico confidencial eran adecuadas. Sin embargo, las salvaguardas adicionales del Código IC no abordaron las debilidades identificadas por el Tribunal en su análisis del régimen del artículo 8 del Convenio, ni cumplían con los requisitos identificados por el Tribunal en los párrafos 448 a 450 anteriores. En particular, no se requería que el uso de selectores o términos de búsqueda que se conocía que estaban conectados a un periodista estuviera autorizado por un juez u otro órgano decisorio independiente u organismo imparcial investido con el poder de determinar si estaba "justificado por un requisito primordial de interés público" y si una medida menos intrusiva podría haber sido suficiente para servir al interés público superior. Por el contrario, cuando la intención era acceder a información periodística confidencial, o era altamente probable en vista del uso de selectores conectados a un periodista, todo lo que se requería era que las razones para proceder de este modo, y la necesidad y proporcionalidad de hacerlo, se documentaran claramente.

457. Además, no existían suficientes salvaguardas para garantizar que una vez que se hiciera evidente que una comunicación que no había sido seleccionada para su examen mediante el uso deliberado de un selector o término de búsqueda conocido por estar conectado con un periodista, sin embargo, contenía información periodística confidencial, sólo podía seguir siendo almacenada y examinada por un analista si estaba autorizado por un juez u otra persona independiente u organismo imparcial de toma de

decisiones investido con el poder de determinar si su almacenamiento y examen continuos estaban "justificados por un requisito primordial de interés público". En cambio, todo lo que requería el párrafo 4.2 del Código IC era que se debía dar "especial consideración" a cualquier interceptación que pudiera haber implicado la interceptación de información confidencial de material periodístico, incluyendo la consideración de cualquier posible medida de mitigación (consultar el párrafo 96 anterior).

458. Teniendo en cuenta tanto estas debilidades como las identificadas por el Tribunal en su examen de la reclamación relativa al artículo 8 del Convenio, considera que también se ha violado el artículo 10 del Convenio en virtud del funcionamiento del régimen de la sección 8 (4).

III. LA RECEPCIÓN DE INTELIGENCIA DE SERVICIOS DE INTELIGENCIA EXTRANJEROS.

A. Artículo 8 del Convenio

459. Los demandantes en el primero de los asuntos acumulados se quejaron de la recepción por parte de las autoridades del Reino Unido de material procedente de servicios de inteligencia extranjeros. Los demandantes en el tercero de los asuntos acumulados alegaron más específicamente que la recepción de material por el Estado demandado interceptado por la NSA bajo PRISM y Upstream violó sus derechos en virtud del artículo 8 del Convenio.

1. Alcance de la reclamación ante la Gran Sala.

460. En el procedimiento *Liberty*, el IPT identificó tres categorías de material que podrían recibirse de socios de inteligencia extranjeros: material de interceptación no solicitado; material de interceptación solicitado; y material no interceptado. Como el Gobierno informó a la Sala que era "inverosímil y raro" que se obtuviera material de interceptación "no solicitado", la Sala no examinó el material que entra en esta categoría (véase el párrafo 417 de la Sentencia de Sala). La Sala también declinó examinar el recibo de material no interceptado, ya que los demandantes no habían especificado el tipo de material que los servicios de inteligencia extranjeros podían obtener por métodos distintos a la interceptación y, como tal, no consideraba que hubieran demostrado que su adquisición interfiriera con sus derechos del artículo 8 (ver apartado 449 de la sentencia de Sala). Los demandantes no han recurrido ninguno de estos fallos.

461. Además, dado que el procedimiento *Liberty* fue iniciado por los demandantes en el tercero de los casos acumulados, el IPT solo consideró la recepción de inteligencia de la NSA. En sus alegaciones ante la Sala y la Gran Sala, las partes también se centraron en la recepción de material de la NSA.

462. Por tanto, la Gran Sala limitará su examen a la reclamación sobre la recepción de material de interceptación solicitado de la NSA.

2. Excepción preliminar del Gobierno.

463. El Gobierno argumentó que los demandantes del primer y tercer asuntos acumulados no podían pretender ser víctimas de una presunta violación porque ninguna de las dos condiciones establecidas en el asunto *Roman Zakharov* (citada anteriormente, §171) se cumplieron (es decir, no era posible que los demandantes hubieran sido

afectados por la legislación que permite medidas de vigilancia secreta, y existían recursos estaban disponibles a nivel nacional). En particular, argumentaron que los demandantes no habían presentado ninguna base que demostrara la existencia de un riesgo real de que sus comunicaciones fueran interceptadas bajo PRISM o Upstream, o de que sus comunicaciones fueran solicitadas por los servicios de inteligencia del Reino Unido. Además, afirmaron que los demandantes tenían a su disposición un recurso interno eficaz para descubrir si fueron objeto de intercambio ilegal de inteligencia.

(a) La sentencia de la Sala.

464. Como la Sala aceptó que el IPT había proporcionado a los demandantes un recurso efectivo para su reclamación acerca del Convenio, consideró que sólo podían pretender ser "víctimas" por la mera existencia del régimen de intercambio de inteligencia si podían demostrar que estaban potencialmente en riesgo de que sus comunicaciones fueran obtenidas por las autoridades de Reino Unido a través de una solicitud a un servicio de inteligencia extranjero (ver párrafos 392 a 393 de la sentencia de la Sala, refiriéndose a *Roman Zakharov*, citada anteriormente, § 171).

465. Con base en la información que se le presentó, la Sala determinó que los demandantes estaban potencialmente en riesgo de que sus comunicaciones fueran obtenidas a través de un servicio de inteligencia extranjero, y solicitadas a éstos por las autoridades del Reino Unido (ver párrafo 395 de la Sentencia de Sala). Aunque solo podían haber requerido la interceptación de sus comunicaciones si existía una orden de la sección 8 (1) o de la sección 8 (4) vigente que cubriera sus comunicaciones, quedó claro en el procedimiento *Liberty* que al menos dos de los demandantes en el tercero de los casos acumulados tuvieron sus comunicaciones legalmente interceptadas y fueron seleccionadas para ser examinadas por los servicios de inteligencia del Reino Unido bajo el régimen de la sección 8 (4). Si bien la Sala no encontró ninguna razón para creer que estos demandantes eran por sí mismos de interés para los servicios de inteligencia, observó que sus comunicaciones podían haber sido obtenidas legalmente bajo el régimen de la sección 8 (4) si, como afirmaron, estaban en contacto con personas que lo fueron. Del mismo modo, sus comunicaciones podían haber sido solicitadas legalmente a un tercer país en virtud del régimen intercambio de inteligencia sí estuvieron en contacto con una persona que fue objeto de una solicitud.

466. Como Upstream funcionaba de manera similar al régimen de la sección 8 (4), la Sala también admitió que las comunicaciones de los demandantes podían potencialmente haber sido obtenidas por la NSA.

(b) Evaluación del Tribunal

467. Los demandantes no han impugnado la conclusión de la Sala de que el IPT ofreció un recurso interno eficaz en relación a las reclamaciones acerca del Convenio sobre el funcionamiento de un régimen de vigilancia, y, por las razones expuestas en los párrafos 413 a 415 anteriores, la Gran Sala está de acuerdo con esa conclusión. Por lo tanto, como observó la Sala, los demandantes solo podían alegar ser "víctimas" debido a la mera existencia del régimen de intercambio de inteligencia si pudieran demostrar que estaban potencialmente en riesgo de que sus comunicaciones fueran obtenidas por las autoridades del Reino Unido a través de una solicitud a un servicio de inteligencia extranjero (ver *Roman Zakharov*, citada anteriormente, § 171). Este solo sería el caso si estuvieran potencialmente en riesgo tanto de que sus comunicaciones fueran

interceptadas por un servicio de inteligencia extranjero como de que dichas comunicaciones fueran solicitadas por la GCHQ.

468. El Gobierno, centrándose en la recepción de información de inteligencia por los Estados Unidos, argumentó que los demandantes no estaban potencialmente en riesgo de que sus comunicaciones fueran interceptadas bajo el programa Upstream, ya que consistía en un régimen de interceptación dirigida. Sin embargo, según la NSA, antes de abril de 2017 Upstream adquirió comunicaciones a, desde o sobre un selector de la sección 702 (como una dirección de correo electrónico); y solo a partir de abril de 2017 en adelante adquirió comunicaciones a o desde un selector de la sección 702 (ver párrafo 263 anterior). Dado que los selectores de la sección 702 se aplicaron a todas las comunicaciones que fluían a través de los cables especificados, parecía que Upstream no era muy diferente al régimen de la sección 8 (4), que también interceptaba todas las comunicaciones que fluían a través de varios cables y las filtraban usando selectores. La única diferencia aparente entre los dos regímenes era que a partir de abril de 2017 la NSA solo podía buscar comunicaciones a o desde un selector fuerte, mientras que la GCHQ mantenía la facultad de realizar búsquedas mediante consultas complejas.

469. En el curso del procedimiento *Liberty*, el IPT confirmó que al menos dos de los demandantes del tercero de los asuntos acumulados no solo habían visto algunas de sus comunicaciones interceptadas de conformidad con una orden la sección 8 (4), sino que también se habían obtenido esas comunicaciones de forma legal y retenido proporcionalmente de conformidad con esa autorización (véanse los párrafos 58 a 60 anteriores). Para que se hubieran retenido legalmente, esas comunicaciones debían haber coincidido con un "selector fuerte" (perteneciente a los demandantes o a alguien con quien estuvieron en contacto) o con una "consulta compleja". El Tribunal considera que, si algunas de las comunicaciones de los demandantes coincidieron con un "selector fuerte" utilizado por la GCHQ, también habrían estado potencialmente en riesgo de ser interceptadas y retenidas por la NSA bajo Upstream en base a que eran "a" o "desde" un selector de la sección 702. Incluso si no coincidían con un selector fuerte, algunas de las comunicaciones de los demandantes podían, sin embargo, haber sido de interés de inteligencia. Antes de abril de 2017, también podían haber sido interceptadas y retenidas por Upstream si fueran "sobre" un selector de la sección 702. Si este fuera el caso, en el momento a valorar (es decir, 7 de noviembre de 2017) esas comunicaciones aún podían haber estado en poder de la NSA ya que, tras el cambio de política en abril de 2017, solo indicó que eliminaría las comunicaciones de Internet adquiridas previamente por Upstream "tan pronto como fuera posible" (véase el párrafo 263 anterior). Por lo tanto, las comunicaciones adquiridas antes de esa fecha que eran "sobre" un selector fuerte podían haber continuado siendo almacenadas por la NSA durante algún tiempo después de eso.

470. En consecuencia, el Tribunal confirma que en el momento temporal a considerar (esto es, el 7 de noviembre de 2017) los demandantes del primer y tercer asuntos acumulados se encontraban en riesgo potencial de que al menos algunas de sus comunicaciones fueran interceptadas y retenidas mediante Upstream.

471. No obstante, los demandantes sólo podían seguir siendo víctimas del régimen de intercambio de inteligencia si también se encontraban con el riesgo potencial de que sus comunicaciones fueran solicitadas por la GCHQ, y tal solicitud solo se podía haber hecho cuando ya existía una orden para el material buscado. Sin embargo, como ya ha

señalado el Tribunal, el hecho de que las comunicaciones de al menos dos de los demandantes en el tercero de los asuntos acumulados fueran retenidas por la GCHQ sugiere que al menos algunas de sus comunicaciones estaban cubiertas por una orden de las previstas en la sección 8(4). En consecuencia, el Tribunal confirma que los demandantes del primer y tercer asuntos acumulados se encontraban en riesgo potencial de que también se solicitaran sus comunicaciones por la GCHQ.

472. En consecuencia, concluye que los demandantes en el primero y tercero de los asuntos acumulados podían reclamar al ser víctimas con respecto a sus reclamaciones sobre el régimen de intercambio de inteligencia. La excepción preliminar planteada por el Gobierno es por tanto desestimada.

3. El fondo.

(a) La sentencia de la Sala.

473. Para considerar el cumplimiento del artículo 8 por parte del régimen que rige la recepción de material interceptado de servicios de inteligencia extranjeros como la NSA, la Sala aplicó una versión modificada de las seis salvaguardas mínimas (véase el párrafo 275). Dado que los dos primeros requisitos no podían aplicarse al solicitar material interceptado a gobiernos extranjeros la Sala a cambio pidió que las circunstancias en las que la interceptación podía ser solicitada estuvieran suficientemente circunscritas para evitar que los Estados usaran esta facultad para eludir las obligaciones de la ley interna o del Convenio. A continuación, aplicó los últimos cuatro requisitos al tratamiento del material interceptado una vez que había sido obtenido por los servicios de inteligencia del Reino Unido.

474. La Sala consideró que el derecho interno, junto con las aclaraciones aportadas por la modificación del Código IC, indicaba con suficiente claridad el procedimiento para solicitar la interceptación o la transferencia de material interceptado de servicios de inteligencia extranjeros. Además, la Sala no encontró evidencias de deficiencias significativas en la aplicación y funcionamiento del régimen. Por lo tanto, se sostuvo por la mayoría, que no ha habido una violación del artículo 8 del Convenio.

(b) Alegaciones de las partes

475. Los demandantes sostuvieron que las salvaguardas vigentes respecto al régimen de intercambio de inteligencia eran inadecuadas. En particular, argumentaron que los problemas que habían llevado a la Sala a apreciar una violación del artículo 8 del Convenio con respecto al régimen de interceptación masiva (es decir, la falta de supervisión del uso de selectores y las salvaguardas inadecuadas con respecto a los datos relacionados con las comunicaciones) se aplicaban igualmente al régimen de intercambio de inteligencia.

476. El Gobierno, en cambio, alegó que el régimen de intercambio de inteligencia tenía una base clara en la legislación nacional, siendo complementado por el Capítulo 12 del Código IC; y dicha ley era accesible. En cuanto a la previsibilidad, el Gobierno argumentó que en lugar de aplicar una versión modificada de las seis salvaguardas mínimas, en cambio, la Sala debería haber aplicado la prueba más general - comúnmente aplicada en casos de recopilación de inteligencia que no implicaran la interceptación de comunicaciones - de si la ley indicaba el alcance de la discrecionalidad y la forma de su ejercicio con suficiente claridad para dar una

protección adecuada al individuo contra injerencias arbitrarias. En cualquier caso, el Gobierno sostuvo que el régimen de intercambio de inteligencia cumplía las seis salvaguardas mínimas. El Código IC describía claramente la naturaleza de los delitos que podían dar lugar a la obtención de información; los límites a la duración de dicha obtención; el proceso para examinar, usar y almacenar la inteligencia obtenida; y las circunstancias en las que la inteligencia debía ser borrada o destruida.

477. Por último, en opinión del Gobierno, no había ninguna buena razón para singularizar las comunicaciones interceptadas y los datos relacionados con las comunicaciones respecto de otro tipo de información que, en principio, podía obtenerse de un servicio de inteligencia extranjero, como inteligencia de fuentes humanas encubiertas o vigilancia audio / visual encubierta. De hecho, en muchos casos, era posible que los servicios de inteligencia ni siquiera supieran si las comunicaciones que les había proporcionado un servicio de inteligencia extranjero habían sido obtenidas como resultado de la interceptación.

(c) Las alegaciones de terceros.

(i) El Gobierno de Francia

478. El Gobierno francés señaló que el intercambio de inteligencia entre los servicios asociados, ya fuera *ad hoc* o de forma periódica, era de vital importancia, especialmente en la lucha contra la creciente transnacionalidad y amenazas difusas que los Estados tenían que prevenir, principalmente identificando sospechosos antes de que actuaran. Esa lucha justificaba el desarrollo de una comunidad de inteligencia, sin la cual los servicios de inteligencia, con su capacidad limitada para actuar en el extranjero, serían incapaces de realizar la tarea que tenían asignada.

479. El Gobierno francés alegó además que en el contexto del intercambio de inteligencia la interferencia no ocurría con la interceptación sino más bien con la obtención de la información, incluso si el material era interceptado a instancias del Estado receptor. Tomó nota del enfoque adoptado por la Sala en el análisis del régimen de intercambio de inteligencia del Reino Unido e invitó a la Gran Sala a adoptar el mismo enfoque.

480. En opinión del Gobierno, la fiabilidad del servicio de recepción era uno de los principales criterios en los que basaba el Estado que enviaba la información su decisión de intercambiar datos y, en consecuencia, el Estado receptor tenía que garantizar la estricta confidencialidad de la información que se le comunicara. Por lo tanto, las garantías requeridas para el manejo de la inteligencia recopilada a través del intercambio de datos con un servicio asociado tenían que estar en consonancia con la "tercera regla del partido", que prohibía a una agencia que había recibido información de un socio extranjero compartirla con un tercero sin el consentimiento de quien la había originado. Sin esa garantía, los Estados podían negarse a transferir la información.

(ii) El Relator Especial de las Naciones Unidas sobre la promoción del derecho a libertad de opinión y expresión.

481. El Relator Especial argumentó que las mismas normas debían ser de aplicación a la adquisición de datos mediante servicios de inteligencia extranjeros que cuando las autoridades nacionales adquirían los datos por sí mismas. Una posición contraria podría llevar a las autoridades estatales a subcontratar *de facto* operaciones de vigilancia

eludiendo así las protecciones otorgadas en el Pacto Internacional de Derechos Civiles y Políticos.

(iii) Access Now.

482. Access Now sostuvo que si bien los tratados de Asistencia Jurídica Mutua ("MLAT") ofrecían un proceso transparente y formal para que un Estado parte pudiera solicitar inteligencia de otro, el uso de programas secretos de inteligencia con señales (por ejemplo, el intercambio de inteligencia de la red Cinco Ojos de la cual el Reino Unido, los Estados Unidos de América, Australia, Canadá y Nueva Zelanda eran miembros) no eran transparentes y estaban prohibidas por las normas internacionales de derechos humanos. Tales programas secretos no eran necesarios, ya que la información de inteligencia que fuera relevante podía obtenerse a través de MLAT.

(iv) Dutch Against Plasterk ("Burgers tegen Plasterk")

483. En Dutch Against Plasterk, una coalición de cinco personas y cuatro asociaciones, eran demandantes en un caso contra los Países Bajos en el que trataron de desafiar el intercambio de datos entre las autoridades holandesas y sus socios de inteligencia extranjeros (incluidos los Estados Unidos y el Reino Unido).

484. En su intervención como tercero ante este Tribunal, la coalición argumentó que el intercambio de inteligencia solo debía permitirse si se acompañaba de las garantías suficientes y la autoridad extranjera tenía una sólida base legal para obtener el material. De lo contrario, podría producirse una elusión de la protección prevista en el artículo 8 del Convenio. No debía permitirse que los Estados obtuvieran material de autoridades extranjeras que no pudiera obtenerse legalmente por sí mismos.

(v) Centro para la Democracia y la Tecnología ("CDT") y Centro Panamericano ("PEN América").

485. El CDT y el PEN América argumentaron que las circunstancias de cooperación internacional en la vigilancia masiva de comunicaciones y datos requerían que se cumplieran al menos tres condiciones: que los Estados evaluaran activamente y se convencieran de la adecuación de los derechos legales y del marco administrativo que rige la interceptación de sus socios extranjeros, y se establecieran estas medidas de adecuación en el derecho interno; que hubiera una autorización independiente – preferiblemente judicial –, basada en el hallazgo de una sospecha razonable, para el uso de selectores identificables a objetivos específicos para consultar la información obtenida de socios extranjeros; y que se requiriera la posterior notificación a los sujetos de la vigilancia.

486. El CDT y el PEN América sostuvieron que los regímenes de interceptación operados por la NSA - en particular, bajo la sección 702 de la FISA y la Orden Ejecutiva 12333 – no satisfacían ni el "de conformidad con la ley" ni los requisitos de "proporcionalidad" del artículo 8 del Convenio, y estas deficiencias mancillaban la legalidad del régimen de intercambio de inteligencia de las leyes del Reino Unido.

(vi) Red europea de instituciones nacionales de derechos humanos ("ENNHRI")

487. La ENNHRI proporcionó ejemplos de Estados contratantes que bajo su punto de vista mostraban que la naturaleza del intercambio de inteligencia internacional había

cambiado significativamente, por lo que se había vuelto difícil distinguir entre datos "solicitados" y "no solicitados". Históricamente, el intercambio internacional había implicado compartir la transferencia de datos evaluados o de información de inteligencia completa. Sin embargo, la llegada de la nueva tecnología había resultado en el aumento de intercambio de datos en "bruto" no evaluados. Incluso cuando había un acuerdo que rigiera la cooperación de inteligencia bilateral o multilateral la llegada de la automatización y los macrodatos hicieron que fuera mucho más desafiante evaluar qué recibió una parte de otra, incluyendo si la información permaneció dentro de los parámetros previstos en la solicitud original. En consecuencia, existía la necesidad de una supervisión independiente sólida del intercambio internacional de inteligencia sin distinción entre datos solicitados y no solicitados. Los órganos de vigilancia deberían tener el mandato legal de supervisar todos los asuntos de cooperación de sus servicios de inteligencia; cooperar con órganos independientes de supervisión de los terceros Estados involucrados en el intercambio de inteligencia; y contratar especialistas independientes, con experiencia en información moderna y tecnología de las comunicaciones, cuando fuera necesario.

(vii) Human Rights Watch ("HRW")

488. Aunque las demandas actuales se centran en la recepción de inteligencia por parte de los Estados Unidos, HRW creía que la red de Estados con los que se compartió comunicaciones de inteligencia era más amplia. Por ejemplo, la Alianza "Cinco Ojos" comprendía a Reino Unido, Estados Unidos, Australia, Canadá y Nueva Zelanda, y también se pensaba que había otras coaliciones de intercambio de inteligencia más restringidas (por ejemplo, los "Nueve ojos", agregando a Dinamarca, Francia, los Países Bajos y Noruega; los "Catorce ojos", agregando a Alemania, Bélgica, Italia, España y Suecia; y los "Cuarenta y un ojos", agregando a otros aliados a la coalición en Afganistán).

(viii) Open Society Justice Initiative ("OSJI")

489. La OSJI argumentó que los Estados no debían recibir ni solicitar datos de un tercero de una forma que eludiera los derechos de las personas previstos en el artículo 8. Para asegurarse de que esto no sucediera, las salvaguardas debían requerirse en el momento en que el material se recopilaba, incluyendo el escrutinio previo de los registros de derechos humanos y leyes y prácticas de interceptación en el Estado extranjero, y la supervisión independiente, preferiblemente judicial, a posteriori de cualquier acuerdo de intercambio para garantizar que las salvaguardas estuvieran establecidas y se hicieran cumplir.

(ix) El Centro de información de privacidad electrónica ("EPIC")

490. El EPIC sostuvo que la ley de los Estados Unidos autorizaba la vigilancia masiva e indiscriminada de personas no estadounidenses. Esta vigilancia tuvo lugar de conformidad con lo previsto en la sección 702 de la FISA y en la Orden Ejecutiva 12333. La vigilancia bajo la sección 702 tuvo lugar en los Estados Unidos con la obligación de asistencia por parte de los proveedores de servicios y se dirigió a personas no estadounidenses quienes se consideraba razonablemente que se encontraban fuera de los Estados Unidos. No había revisión judicial previa de la actividad de vigilancia; no se requería sospecha razonable; y no existía la obligación legal de notificar a los sujetos de la vigilancia. Todo lo que se requería era que el FISC revisara anualmente los

procedimientos de selección y minimización destinados a limitar la adquisición de comunicaciones de personas estadounidenses o personas ubicadas en los Estados Unidos.

491. La Orden Ejecutiva 12333 autorizó a la NSA a adquirir inteligencia y contrainteligencia. La orden otorgó amplias facultades para realizar vigilancia de inteligencia de señales de una amplia variedad de fuentes, incluyendo las redes de fibra óptica. La recolección se llevó a cabo fuera del territorio de los Estados Unidos. No había informes ni divulgaciones oficiales sobre el alcance de la vigilancia en virtud de la orden, la cual no estaba sujeta a vigilancia.

492. En opinión del EPIC, la vigilancia por parte de la NSA violaría el artículo 8 del Convenio por no limitar el ámbito de aplicación ni la duración, así como por la falta de supervisión, notificación y recursos adecuados.

(x) La Comisión Internacional de Juristas ("CIJ")

493. La CIJ remitió al Tribunal a los artículos 15 y 16 de los Artículos de responsabilidad estatal de la Comisión de Derecho Internacional ("los Artículos de la CDI"). La misma sostuvo que, de conformidad con el artículo 15, el Estado contratante podía ser responsable de la vigilancia masiva realizada por un Estado no contratante si actuaban de forma organizada y mediante una cooperación estructurada; y que, de conformidad con el artículo 16, un Estado Contratante podía ser responsable de la vigilancia masiva realizada por un Estado no contratante si contribuyó al programa de vigilancia y obtuvo resultados reales o tuvo conocimiento implícito de las violaciones de las obligaciones internacionales de derechos humanos inherentes al sistema. La CIJ consideró además que los Estados contratantes que participasen o contribuyeran a un programa de vigilancia masiva debían estar obligados a establecer un sistema de salvaguardas para la protección de los derechos del artículo 8, y también tenían el deber de proteger a las personas dentro de su jurisdicción de las violaciones de los derechos del artículo 8 causadas por programas de vigilancia masiva.

(xi) Sociedad de Derecho de Inglaterra y Gales

494. La Sociedad de Derecho sostuvo que el régimen del artículo 8 (4) y los códigos asociados no proporcionaron salvaguardas sólidas o transparentes para el material legalmente privilegiado. Dado que se aplicaban las mismas salvaguardas al material privilegiado obtenido por Estados extranjeros y divulgado a los servicios de inteligencia del Reino Unido, las mismas deficiencias también contaminaron este régimen.

(d) Evaluación del Tribunal

(i) El test aplicable

495. En opinión de la Sala, la interceptación de comunicaciones por los servicios de inteligencia extranjeros no podía implicar la responsabilidad de un Estado receptor, o estar dentro de la jurisdicción de ese Estado en el sentido del artículo 1 del Convenio, incluso si la interceptación se llevó a cabo a petición del Estado (ver párrafo 420 de la sentencia de la Sala). En primer lugar, en la medida en que algunos de los terceros intervinientes habían invocado los artículos de la CDI, la Sala consideró que estos solo serían aplicables si los servicios de inteligencia extranjeros se pusieron a disposición del Estado receptor y actuaban en ejercicio de elementos de la autoridad gubernamental de

ese Estado (artículo 6); si el Estado receptor ayudó o asistió a los servicios de inteligencia extranjeros en la interceptación de las comunicaciones cuando constituía un hecho internacionalmente ilícito para el Estado responsable de los servicios, el Estado receptor era consciente de la circunstancia de que el acto era internacionalmente ilícito, y el acto hubiera sido internacionalmente ilícito si lo cometiese el Estado receptor (artículo 16); o si el Estado receptor ejerció dirección o control sobre el gobierno extranjero (artículo 17). En segundo lugar, según la jurisprudencia del Tribunal, la interceptación de comunicaciones de un servicio de inteligencia extranjero solo caería dentro de la jurisdicción del Estado receptor si ese Estado estaba ejerciendo autoridad o control sobre el servicio de inteligencia extranjero (ver, por ejemplo, *Al-Skeini y otros contra el Reino Unido* [GC], núm. 55721/07, §§ 130-139, TEDH 2011 y *Jaloud contra los Países Bajos* [GC], núm. 47708/08, §§ 139 y 151 TEDH 2014).

496. La Gran Sala coincide con la Sala en que ninguno de estos elementos estaba presente en la situación considerada y, de hecho, en sus alegatos ante la Gran Sala, los demandantes no han sugerido que lo estuvieran. Por tanto, cualquier injerencia en el artículo 8 del Convenio solo podía residir en la solicitud inicial y en la posterior recepción del material interceptado, seguido de su posterior almacenamiento, examen y uso por parte de los servicios de inteligencia del Estado receptor.

497. La protección otorgada por el Convenio devendría ineficaz si los Estados pudieran eludir las obligaciones del Convenio solicitando la interceptación de las comunicaciones o la transmisión de comunicaciones interceptadas de Estados no contratantes; o incluso, aunque no ocurrió directamente en los casos que nos ocupan, al obtener tales comunicaciones a través del acceso directo a las bases de datos de esos Estados. Por lo tanto, en opinión del Tribunal, cuando se solicita a un Estado no contratante material interceptado, la solicitud debe tener su base en la legislación interna, y la ley debe ser accesible a la persona interesada y previsible en cuanto a sus efectos (véase *Roman Zakharov*, citada anteriormente, § 228). También será necesario disponer de normas claras y detalladas que den a los ciudadanos una indicación adecuada de las circunstancias y las condiciones en las que las autoridades se encuentran facultadas para hacer tal solicitud (ver *Roman Zakharov*, citada anteriormente, § 229; *Malone*, citada anteriormente, § 67; *Leander*, antes citada, § 51; *Huvig*, citada anteriormente, § 29; *Kruslin*, antes citada, § 30; *Valenzuela Contreras*, antes citada, § 46; *Rotaru*, citada anteriormente, § 55; *Weber y Saravia*, antes citada, § 93; y *Asociación para la Integración Europea y los Derechos Humanos y Ekimdzhiev*, citada anteriormente, § 75) y que brindan garantías efectivas contra el uso de este poder para eludir la legislación nacional y / o las obligaciones de los Estados en virtud del Convenio.

498. Al recibir el material interceptado, el Tribunal considera que el Estado receptor debe disponer de las salvaguardas adecuadas para su examen, uso y almacenamiento; para su ulterior transmisión; y para su borrado y destrucción. Estas salvaguardas, desarrolladas por primera vez por el Tribunal en su jurisprudencia sobre la interceptación de comunicaciones por los Estados contratantes, son igualmente aplicables a la recepción, por un Estado Contratante, de material interceptado que haya sido solicitado a servicio de inteligencia extranjero. Si, como sostiene el Gobierno, los Estados no siempre saben si el material recibido de servicios de inteligencia extranjeros es resultado de la interceptación, entonces el Tribunal considera que habrían de aplicarse las mismas normas a todo el material recibido de servicios de inteligencia extranjeros que pudiera ser resultado de la interceptación.

499. Finalmente, el Tribunal considera que cualquier régimen que permita a los servicios de inteligencia solicitar la interceptación o interceptar material de Estados no contratantes, o acceder directamente a dicho material, debería estar sujeto a supervisión independiente, y también debería existir la posibilidad de una revisión *ex post facto* independiente.

(ii) Aplicación de ese test al caso que nos ocupa.

500. El acuerdo sobre comunicaciones de inteligencia entre el Reino Unido y los Estados Unidos de 5 de marzo 1946 permitía específicamente el intercambio de material entre los Estados Unidos y el Reino Unido (véase el párrafo 103 anterior). Sin embargo, los detalles de las disposiciones internas de los servicios de inteligencia (o "por debajo de la línea de flotación") sólo fueron revelados durante el procedimiento *Liberty* (ver párrafos 33 a 36 anteriores). Esta nueva información se incorporó posteriormente al Capítulo 12 del Código IC (véase el párrafo 116 anterior) que, como ya se apuntó, era un documento público, sujeto a la aprobación de ambas Cámaras del Parlamento, y que ha de ser tenido en cuenta tanto por los que ejercen funciones de interceptación como por los jueces y tribunales (ver párrafos 93-94 anteriores). El Tribunal ha aceptado que las disposiciones del Código IC podían tenerse en cuenta al evaluar la previsibilidad del régimen de la RIPA (ver *Kennedy*, citada anteriormente, § 157 y párrafo 366 anterior) y que el mismo debe necesariamente aplicarse al régimen de intercambio de inteligencia.

501. En consecuencia, el Tribunal considera que el régimen de solicitud y recepción de inteligencia por parte de Estados no contratantes tenía una base clara en el derecho interno y, a raíz de la enmienda al Código IC, esa ley 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 los ciudadanos, el Tribunal ahora - de acuerdo con su habitual metodología (véase el párrafo 334 anterior) – procederá a evaluar, conjuntamente, la previsibilidad y la necesidad del régimen de intercambio de inteligencia.

502. El capítulo 12 del Código IC (véase el párrafo 116 anterior) sigue al mismo enfoque que el adoptado por la legislación nacional con respecto a los productos de la interceptación masiva. Según el Capítulo 12, los servicios de inteligencia solo podían hacer una solicitud a un gobierno extranjero para interceptar comunicaciones y / o datos asociados a las comunicaciones no analizados si la pertinente orden de interceptación exigida por la RIPA ya había sido emitida por el Secretario Estado, la ayuda del gobierno extranjero era necesaria para obtener esas comunicaciones en particular porque no se podían obtener bajo una orden existente (véase el párrafo 12.2 del Código IC en el párrafo 116 anterior), y era necesario y proporcionado para la agencia interceptora obtener esas comunicaciones. A estos efectos, una orden pertinente de interceptación significaba una orden de la sección 8(1) de la RIPA en relación con el tema en cuestión; una orden de la sección 8(4) y un certificado adjunto que incluyera una o más "descripciones del material interceptado" que cubrieran las comunicaciones del sujeto; o, cuando se sabía que el sujeto estaba dentro las Islas Británicas, una orden conforme a la sección 8(4) y un certificado adjunto que incluyera una o más "descripciones del material interceptado" que cubriera sus comunicaciones, junto con la modificación apropiada conforme a la sección 16(3).

503. Cuando existieran circunstancias excepcionales, la solicitud de las comunicaciones podía hacerse en ausencia de una orden de interceptación de la RIPA solo si no equivalía a una elusión deliberada de la RIPA o frustraba de otra manera sus objetivos (por ejemplo, porque no fuera técnicamente factible obtener las comunicaciones a través de la interceptación de la RIPA), y fuera necesario y proporcionado obtener esas comunicaciones por la agencia de interceptación. En tal caso, la solicitud tenía que ser considerada y decidida por el Secretario de Estado personalmente, y, de conformidad con el Código IC conforme fue modificado, notificado al Comisionado IC. Según la información divulgada durante el proceso de *Liberty*, y confirmada en las alegaciones del Gobierno ante la Sala y la Gran Sala, nunca se ha realizado ninguna solicitud de material interceptado en ausencia de una orden de la RIPA (ver párrafo 42 anterior).

504. A la luz de lo anterior, el Tribunal considera que el derecho interno establece normas jurídicas claras que dan a los ciudadanos una indicación adecuada de las circunstancias y las condiciones en las que las autoridades podían solicitar material interceptado por un Estado extranjero.

505. Cuando se disponía de una orden pertinente de la sección 8 (1) o de la sección 8 (4), esa orden había sido autorizada por el Secretario de Estado. Más concretamente, se desprende del párrafo 12.5 de la Código IC, leído junto con la nota al pie que la acompaña, que cuando una solicitud se basaba en una orden existente la solicitud se haría a, de o sobre selectores específicos (es decir, relacionados con individuo/s específico/s) y el Secretario de Estado ya habría aprobado la solicitud de las comunicaciones de esas personas. Mientras que, en circunstancias excepcionales, se podía realizar una solicitud en ausencia de una orden pertinente, el Secretario de Estado tenía que aprobar personalmente la solicitud y, si se basaba en selectores específicos, tenía personalmente que considerar y aprobar el examen de esas comunicaciones con referencia a esos factores (véase párrafo 116 anterior).

506. De acuerdo con la legislación nacional, en relación con las solicitudes para el intercambio de inteligencia, debe darse el mismo enfoque que en la interceptación masiva, y como la legislación nacional disponía explícitamente que no debía haber elusión, no es necesario que el Tribunal examine por separado el procedimiento de autorización.

507. En cuanto a las salvaguardas para el examen, uso, almacenamiento, transmisión, borrado y destrucción del material interceptado solicitado, estaban claras en el párrafo 12.6 del Código IC el contenido o datos relacionados con las comunicaciones obtenidas por los servicios de inteligencia del Reino Unido o de otro Estado, que se identificaran como producto de la interceptación, tenían que estar sujetos a las mismas reglas internas y salvaguardas que eran de aplicación a las mismas categorías de contenido o datos cuando se obtuvieran directamente por las agencias interceptoras como resultado de una interceptación bajo la RIPA. En consecuencia, las salvaguardas previstas en las secciones 15 y 16 de la RIPA, complementadas por el Código IC, se aplicaban igualmente a la interceptación de comunicaciones y datos de las comunicaciones obtenidos de servicios de inteligencia, siempre que el material “se identificara como producto de la interceptación”.

508. El Tribunal ha examinado las salvaguardas de las secciones 15 y 16 en relación al régimen de interceptación masiva y concluyó que los procedimientos para almacenar,

acceder, examinar y utilizar el material adquirido; para comunicar el material a otras partes; y para el borrado y destrucción del material obtenido eran suficientemente claros y brindaban una protección adecuada contra el abuso (véanse los párrafos 384 a 405 anteriores). A la luz de las conclusiones del Tribunal en el párrafo 498 anterior, se señala que el párrafo 12.6 del Código IC no extiende las salvaguardas previstas en las secciones 15 y 16 de la RIPA, complementadas por el Código IC, a todo el material recibido de servicios de inteligencia extranjeros que pudieran ser producto de la interceptación, limita estas salvaguardas solo al material que se identifique como tal; sin embargo, el Tribunal no considera que este hecho por sí solo determine el incumplimiento del artículo 8 por parte del régimen de intercambio de inteligencia.

509. En el contexto del régimen de la sección 8 (4), al Tribunal le preocupaba la exención de las salvaguardas del artículo 16 respecto a los datos relacionados con las comunicaciones. Sin embargo, bajo el régimen de la sección 8 (4), el Estado pudo interceptar, almacenar y buscar todos los paquetes de comunicaciones que viajaban a través ciertos portadores. La exención general de las salvaguardas de la sección 16 a los datos relacionados con las comunicaciones significaba que todos estos datos, independientemente de si eran de algún interés de inteligencia, podían ser registrados por los servicios de inteligencia aparentemente sin restricciones. Bajo el Capítulo 12 del Código IC, por otro lado, no eran solicitados el contenido y los datos relacionados con las comunicaciones por los servicios de inteligencia en masa. El párrafo 12.5 del Código IC, junto con la nota a pie que lo acompaña, indica que cuando la solicitud se base en una orden existente dicha solicitud debería ser hecha a, de o sobre selectores específicos (es decir, individuos específicos) y cuando el Secretario de Estado ya haya aprobado la solicitud de comunicaciones de esos individuos. Mientras que en circunstancias excepcionales la solicitud podía hacerse en ausencia de una orden, el Secretario de Estado tenía que aprobar personalmente la solicitud y, si se basaba en selectores específicos, tenía que considerar personalmente 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 atribuible a una persona conocida por estar en el Islas Británicas a menos que el Secretario de Estado hubiera aprobado el examen de esas comunicaciones (véase el párrafo 116 anterior). En otras palabras, los servicios de inteligencia solicitaban inteligencia relacionada con un individuo para quienes el Secretario de Estado ya había considerado la necesidad y proporcionalidad de la obtención de sus comunicaciones; o la salvaguarda de la sección 16 era aplicable al material obtenido. Como ninguna solicitud se ha hecho sin una orden, parece que, hasta la fecha, todas las solicitudes han caído en la primera categoría.

510. Por tanto, el Tribunal considera que el Reino Unido tenía establecidas salvaguardas adecuadas para el examen, uso y almacenamiento del contenido y datos de las comunicaciones recibidos de sus socios de inteligencia; para la transmisión ulterior de este material; y para su borrado y destrucción.

511. Finalmente, el Tribunal observó que el Comisionado IC y el IPT proporcionaban una capa adicional de protección (ver párrafo 41 anterior). El Comisionado IC supervisó el régimen de intercambio de inteligencia: el párrafo 12.7 del Código IC (ver párrafo 116 anterior) requería que le fueran notificadas todas las solicitudes realizadas en ausencia de una orden, y supervisó el otorgamiento de órdenes y el almacenamiento del material por parte de los servicios de inteligencia.

512. Además de la supervisión del Comisionado IC, el IPT proporcionaba una revisión *ex post facto* del régimen de intercambio de inteligencia. Como puede verse desde los procedimientos de *Liberty*, el IPT estaba abierto a cualquiera que deseara plantear una reclamación específica o general sobre el régimen de intercambio de inteligencia; y, en respuesta, el IPT podía examinar tanto las disposiciones "por encima de la línea de flotación" como "por debajo de la línea de flotación" en orden a evaluar el cumplimiento del régimen del Convenio.

513. En consecuencia, el Tribunal considera que el régimen de solicitud y recepción del material interceptado era compatible con el artículo 8 del Convenio. Existían reglas claras y detalladas que daban a los ciudadanos indicaciones adecuadas de las circunstancias y las condiciones en las que las autoridades estaban facultadas para hacer una solicitud a un servicio de inteligencia extranjero; la legislación nacional contenía garantías efectivas contra el uso de dichas solicitudes con el fin de eludir la ley nacional y / o las obligaciones del Reino Unido en virtud del Convenio; el Reino Unido tenía establecidas las protecciones adecuadas para el examen, uso, almacenamiento, ulterior transmisión, borrado y destrucción del material; el régimen estaba sujeto a supervisión independiente por parte del Comisionado IC y existía la posibilidad de revisión *ex post facto* por parte del IPT.

514. En consecuencia, no se ha producido una violación del artículo 8 del Convenio.

B. Artículo 10 del Convenio

515. Los demandantes en el tercero de los asuntos acumulados también se quejaron de que el régimen de intercambio de inteligencia había violado sus derechos en virtud del artículo 10 del Convenio. En la medida en que dicha reclamación se refería a 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 para su consideración en el procedimiento interno (ver párrafo 473 de la sentencia de la Sala). Por tanto, este aspecto de la reclamación queda fuera del alcance del examen de la Gran Sala.

516. Los demandantes en el tercero de los asuntos acumulados también se quejaron de manera más general sobre el cumplimiento por el régimen de intercambio de inteligencia del artículo 10. Aunque este argumento fue planteado ante el IPT en su debido momento, el Tribunal coincide con la Sala en que no da lugar a ninguna cuestión distinta a las que se derivan del artículo 8 del Convenio (véase párrafo 474 de la sentencia de la Sala). Por tanto, considera que tampoco se ha producido una violación del artículo 10 del Convenio.

IV. ADQUISICIÓN DE DATOS DE COMUNICACIONES DE PROVEEDORES DE SERVICIOS DE COMUNICACIONES

A. Artículo 8 del Convenio

517. Los demandantes en el segundo de los casos acumulados se quejaron de que el régimen para la adquisición de datos de comunicaciones bajo el Capítulo II de la RIPA era incompatible con sus derechos en virtud del artículo 8 del Convenio.

1. La sentencia de la Sala

518. A la fecha del examen del caso por la Sala, el Gobierno del Reino Unido estaba en proceso de reemplazar el marco legal existente para llevar a cabo la vigilancia secreta por la nueva IPA. Las disposiciones de la nueva legislación que rigen la retención de los datos de comunicaciones por los CSPs estaban sujetas a un desafío legal interno por *Liberty*. En el curso de ese procedimiento, el Gobierno reconoció que las disposiciones aplicables eran incompatibles con los requisitos de la legislación de la UE. En consecuencia, el Tribunal Superior consideró que la Parte 4 era incompatible con los derechos fundamentales reconocidos en la legislación de la UE ya que, en el ámbito de la justicia penal, el acceso a los datos retenidos no se limitaba al fin de combatir "delitos graves"; ni estaba sujeto a una revisión previa por parte de un tribunal o de un organismo administrativo independiente (véase el párrafo 190 anterior).

519. Habida cuenta de la primacía del derecho de la UE sobre el derecho del Reino Unido, y la confirmación del Gobierno en el proceso interno de que el disposiciones de la IPA que rigen la retención de datos de comunicaciones por parte de los CSPs eran incompatibles con la legislación de la UE, la Sala consideró "claro" que la legislación nacional exigía que cualquier régimen que permitiera a las autoridades acceder los datos retenidos por los CSPs debía limitar el acceso al fin de combatir "delitos graves", y que el acceso debía estar sujeto a revisión previa por parte de un tribunal u organismo administrativo independiente. Como el régimen predecesor sufría de los mismos "defectos" que su sucesora, la Sala consideró que no podía ser conforme a la ley en el sentido del artículo 8 del Convenio (véanse párrafos 465 a 468 de la sentencia de la Sala).

2. Alegaciones de las partes

520. Las partes no hicieron más alegaciones ante la Gran Sala con respecto a esta reclamación.

3. Evaluación del Tribunal

521. El Gobierno no impugnó las conclusiones de la Sala ante la Gran Sala. Además, este último no encuentra ningún fundamento para no estar de acuerdo con la conclusión de la Sala.

522. En consecuencia, el Tribunal considera que en el presente caso se produjo una violación del artículo 8 del Convenio por el hecho de que la actuación conforme al régimen bajo el Capítulo II de la RIPA no fue "de conformidad con la ley".

B. Artículo 10 del Convenio.

523. Los demandantes en el segundo de los casos acumulados también se quejaron en virtud del artículo 10 de la Convención del régimen de adquisición de datos de las comunicaciones a través de los CSPs.

1. La sentencia de la Sala

524. La Sala reconoció que el régimen del Capítulo II otorgaba una protección mejorada cuando los datos se solicitaban con el fin de identificar una fuente de un periodista. En particular, el párrafo 3.77 del Código de prácticas de adquisición datos de comunicaciones establecía que siempre y cuando una solicitud pretendiera determinar una fuente de información periodística, debía haber un requisito primordial de interés

público, y tales solicitudes tenían que regirse por los procedimientos de la Ley de Policía y Evidencia Criminal de 1984 ("PACE") y solicitar a un tribunal una orden para obtener estos datos. De conformidad con el Anexo 1 de la PACE, se enviaba una solicitud para la emisión de una orden a un juez y, cuando la solicitud se refiriera a material que consistiera o incluyera material periodístico, la solicitud debía hacerse *inter partes*. La autorización interna sólo podía utilizarse si se creía que había una amenaza inmediata de pérdida de vida humana, y la vida de esa persona podía estar en peligro por la dilación inherente al proceso de autorización judicial (véase el párrafo 498 de la sentencia de la Sala).

525. No obstante, estas disposiciones solo se aplicaban cuando el fin de la solicitud era determinar una fuente; no aplicaban en todos los casos donde hubo una solicitud de los datos de la comunicación de un periodista, o cuando era probable tal intrusión colateral. Además, en los casos relacionados con el acceso a los datos de la comunicación de un periodista no había ninguna disposición especial que restringiera el acceso con el fin de combatir los "delitos graves". En consecuencia, la Sala consideró que el régimen no era "de conformidad con la ley" a los efectos de la reclamación relativa al artículo 10 (véase apartados 496 a 499 de la sentencia de la Sala).

2. Alegaciones de las partes

526. Las partes no hicieron más alegaciones ante la Gran Sala con respecto a esta reclamación.

3. Evaluación del Tribunal

527. El Gobierno no impugnó las conclusiones de la Sala ante la Gran Sala. Además, esta última no encuentra ningún fundamento para no estar de acuerdo con las conclusiones de la Sala.

528. En consecuencia, el Tribunal considera que en el presente caso se ha producido asimismo una violación del artículo 10 del Convenio dado que el funcionamiento del régimen del Capítulo II de la RIPA no era "conforme con la ley".

V. APLICACIÓN DEL ARTÍCULO 41 DEL CONVENIO

529. El artículo 41 del Convenio dispone:

> "Si el Tribunal declara que ha habido violación del Convenio o de sus Protocolos y si el derecho interno de la Alta Parte Contratante sólo permite de manera imperfecta reparar las consecuencias de dicha violación, el Tribunal concederá a la parte perjudicada, si así procede, una satisfacción equitativa."

A. Daño

530. Los demandantes no presentaron ninguna reclamación con respecto a daños materiales o daños morales. En consecuencia, el Tribunal considera que no es necesario concederles cantidad alguna por estos conceptos.

B. Costas y gastos.

531. Ante la Sala los demandantes del primero de los asuntos acumulados reclamaron la cantidad de 208.958,55 libras esterlinas en relación a sus costas y gastos; y los demandantes en el segundo de los asuntos acumulados reclamaron la cantidad de

45.127,89 libras esterlinas. Los demandantes del tercero de los asuntos acumulados no presentaron ninguna reclamación en concepto de costas y gastos.

532. La Sala otorgó a los demandantes en el primero de los casos acumulados la cantidad de 150.000 euros; y a los demandantes en el segundo de los asuntos acumulados la suma de 35.000 euros.

533. Ante la Gran Sala los demandantes en el primero de los asuntos acumulados reclamaron otras 138.036,66 libras esterlinas; los demandantes en el segundo de los asuntos acumulados reclamaron otras 69.200,20 libras esterlinas; y los demandantes en el tercero de los asuntos acumulados reclamaron 44.993,60 libras esterlinas.

534. El Gobierno impugnó la cuantía reclamada.

535. Según la jurisprudencia del Tribunal, el demandante tiene derecho al reembolso de las costas y gastos solo en la medida en que se haya demostrado que éstos han sido reales y necesarios y su cantidad sea razonable. En el presente caso, teniendo en cuenta los documentos presentados y los criterios anteriores, el Tribunal considera razonable otorgar las siguientes sumas que cubren los gastos de todos los costes del procedimiento ante la Sala: a los demandantes en el primero de los asuntos acumulados la suma de 150.000 euros; y a los demandantes en el segundo de los asuntos acumulados la suma de 35.000 euros. También considera razonable otorgar las siguientes sumas que cubren los gastos de todos los costes de los procedimientos ante la Gran Sala: a los demandantes en el primero de los asuntos acumulados, la suma de 77.500 euros; a los demandantes en el segundo de los asuntos acumulados, la suma de 55.000 euros; y a los demandantes en el tercero de los asuntos acumulados, la suma de 36.000 euros.

C. Interés de demora

536. El Tribunal considera apropiado que el interés de demora se calcule con base al tipo de interés marginal de los préstamos del Banco Central Europeo, al que habría que añadirse tres puntos porcentuales.

POR CUANTO ANTECEDE, ESTE TRIBUNAL

1. *Declara*, por unanimidad, que se ha producido una violación del artículo 8 del Convenio con respecto al régimen de la sección 8(4);

2. *Declara*, por unanimidad, que se ha producido una violación del artículo 8 del Convenio con respecto al régimen del Capítulo II;

3. *Declara*, por doce votos contra cinco, que no ha habido violación del artículo 8 del Convenio con respecto a la recepción de información de los de servicios de inteligencia extranjeros;

4. *Declara*, por unanimidad, que, en la medida en que fue planteada por los demandantes en el segundo de los casos acumulados, ha habido una violación del artículo 10 del Convenio con respecto al régimen de la sección 8(4) y el régimen del Capítulo II.

5. *Declara*, por doce votos contra cinco, que no ha habido violación del Artículo 10 del Convenio con respecto a la recepción de información de los de servicios de inteligencia extranjeros;

6. *Declara*, por unanimidad,

(a) que el Estado demandado ha de pagar a los demandantes, en un plazo de tres meses, las siguientes cantidades, que serán convertidas a la moneda del Estado demandado conforme a la tasa aplicable a la fecha de liquidación:

(i) a los demandantes del primero de los asuntos acumulados: 227.500 euros (doscientos veintisiete mil quinientos euros), más cualquier impuesto que pudiera devengarse para los demandantes, en concepto de costas y gastos;

(ii) a los demandantes del segundo de los asuntos acumulados: 90.000 euros (noventa mil euros), más cualquier impuesto que pudiera devengarse para los demandantes, en concepto de costas y gastos;

(iii) a los demandantes del tercero de los asuntos acumulados: 36.000 euros (treinta y seis mil euros), más cualquier impuesto que pudiera devengarse para los demandantes, en concepto de costas y gastos;

(b) que desde la expiración de los tres meses antes mencionados será pagadero el interés simple de liquidación sobre los montos anteriores a una tasa igual a la tasa de interés marginal de los préstamos del Banco Central Europeo durante el período de incumplimiento más tres puntos porcentuales;

7. *Rechaza*, por unanimidad, el resto de reclamaciones de los demandantes por satisfacción equitativa.

Redactada en francés e inglés y pronunciada en audiencia el 25 de mayo 2021, de conformidad con a las Reglas 77. 2 y 3 del Reglamento del Tribunal.

Søren Prebensen — Adjunto al Secretario

Robert Spano — Presidente

De conformidad con el artículo 45.2 del Convenio y la regla 74.2 del Reglamento del Tribunal, se adjuntan a la presente sentencias los siguientes votos particulares:

a) Voto particular conjunto parcialmente concurrente de los Magistrados Lemmens, Vehabović y Bošnjak;

(b) Voto particular parcialmente concurrente y parcialmente disidente del juez Pinto de Albuquerque;

c) Voto particular conjunto parcialmente disidente de los Magistrados Lemmens, Vehabović, Ranzoni y Bošnjak.

R.S.O.

S.C.P.

VOTO PARTICULAR CONJUNTO PARCIALMENTE CONCURRENTE DE LOS JUECES LEMMENS, VEHABOVIĆ Y BOŠNJAK

1. En el caso que nos ocupa, coincidimos con la mayoría en todos los puntos del fallo de la Sentencia, salvo el punto 3 (no violación del artículo 8 del Convenio con respecto a la recepción de información de inteligencia de servicios de inteligencia extranjeros) y 5 (no violación del artículo 10 del Convenio en relación a la recepción de información de inteligencia procedente de servicios inteligencia extranjeros). Para mostrar en qué no estamos de acuerdo con el resultado del caso, presentamos un voto particular conjunto con nuestro colega el Juez Ranzoni. Además, presentamos este voto particular concurrente para subrayar que, si bien la presente sentencia en su conjunto está elegantemente estructurada y es en gran parte clara en su mensaje, también ha perdido una excelente oportunidad para defender plenamente la importancia de la vida privada y la correspondencia ante la interferencia en forma de vigilancia masiva.

I. OBSERVACIONES INTRODUCTORIAS

2. Este caso consiste en un ejercicio de equilibrio en el que los intereses legítimos perseguidos por los Estados contratantes deben sopesarse frente a los derechos humanos y libertades fundamentales, en particular los protegidos por el artículo 8 del Convenio. Al inicio de su evaluación (párrafos 322 y 323 de la sentencia), la Gran Sala describe extensamente la naturaleza de las amenazas modernas a las que se enfrentan los Estados contratantes y reconoce lo valiosa que la interceptación masiva puede ser en la identificación y prevención de esas amenazas. Además, la sentencia subraya la necesidad de mantener el secreto de las operaciones en esta materia que considera legítimo, lo que significa que poco o nada de la información sobre un procedimiento determinado estará disponible para el público. Mientras uno puede suscribir, en cierta medida, esta descripción del interés legítimo para operar mediante un régimen de intercepción masiva, no hay un énfasis similar sobre la importancia de la privacidad o cualquier otro interés privado en esas mismas observaciones preliminares. Aunque lo anterior no guarda relación directa con la evaluación del sistema de interceptación masiva bajo escrutinio, habríamos preferido una introducción más equilibrada respecto a esta evaluación.

3. Antes de entrar en el análisis de lo que consideramos los puntos débiles de la presente sentencia, vale la pena recordar que la privacidad es una condición previa fundamental no solo para una variedad de intereses individuales fundamentales, sino también para la existencia de una sociedad democrática. Es esencial para el bienestar, la autonomía, el autodesarrollo y la capacidad de la persona para mantener relaciones significativas con otras personas. También es una condición previa necesaria para el disfrute de los derechos civiles y, en consecuencia, para ostentar la condición de persona como miembro libre e igualitario de una sociedad democrática. Las invasiones a la privacidad no solo disminuyen la autonomía individual y la salud mental y física, sino que también inhiben el autogobierno democrático.

4. Primero, la privacidad es importante para la salud física y mental de una persona. El mero sentimiento de que uno está siendo observado y evaluado constantemente por otros puede tener efectos graves en el bienestar físico y mental. Eso hace que los individuos internalicen demasiado su comportamiento social, de modo que se sientan culpables o avergonzados por cualquier sentimiento o pensamiento, deseo o prácticas

que no querrían expresar públicamente. Tales tensiones entre las exigencias de su vida interior y las presiones de la presentación de uno mismo pueden provocar graves problemas de salud.

5. En segundo lugar, la observación externa y las presiones sobre la presentación de uno mismo puede obstruir "la promoción de la libertad, la autonomía, la individualidad, las relaciones y el fomento de la existencia de una sociedad libre"[1]. La vigilancia inhibe porque disminuye la medida en que podemos espontáneamente relacionarnos de todo corazón con otras personas y participar en determinadas actividades. La falta de privacidad tendría un efecto sofocante en nuestra vida interior, nuestras relaciones y, en última instancia, nuestra autonomía. "Así se perderá ... el núcleo interior personal que es la fuente de la crítica del Convenio, la creatividad, la rebelión y la renovación"[2].

6. En tercer lugar, la 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 total y darle la apariencia de legitimidad, existe el peligro inherente de que el Estado utilice la vigilancia para garantizar el cumplimiento y el conformismo. Como describió George Orwell en la novela mil novecientos ochenta y cuatro:

> "Por supuesto, no había manera de saber si le contemplaban a uno en un momento dado. Lo único posible era figurarse la frecuencia y el plan que empleaba la Policía del Pensamiento para controlar un hilo privado. Incluso se concebía que los vigilaran a todos a la vez. Pero, desde luego, podían intervenir su línea cada vez que se les antojara. Tenía usted que vivir —y en esto el hábito se convertía en un instinto— con la seguridad de que cualquier sonido emitido por usted sería registrado y escuchado por alguien y que, excepto en la oscuridad, todos sus movimientos serían observados."[3]

7. Al asegurar un reino para la actividad no observada, la privacidad fomenta la autonomía moral de los ciudadanos, un requisito central del autogobierno en las democracias[4]. Solo los seres autónomos pueden gobernar verdaderamente ellos mismos y sólo los seres autónomos pueden gozar verdaderamente de todos los derechos civiles, tales como el derecho al voto, la libertad de asociación y participación en la sociedad civil, las libertades de pensamiento y conciencia, de palabra y de expresión, y la libertad de religión, que son esenciales para el autogobierno. No podemos decir que disfrutamos plenamente de las libertades que se supone que estos derechos nos otorgan si nuestra libertad interior está comprometida.

8. Pero la vigilancia no se limita a ejercer presiones internas sobre la libertad. En la medida en que los ciudadanos conservan su autonomía, ésta también ejerce presiones sobre su libertad para ejercer sus derechos civiles. Así como vivir bajo el control social constante nos hace menos propensos a actuar de acuerdo con nuestros sentimientos y pensamientos por miedo al ostracismo, vivir bajo la vigilancia constante del gobierno puede hacer que los ciudadanos sean un poco más cautelosos al comprometerse 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

[1] Ruth Gavison (1980), "Privacidad y los límites de la ley", Yale Law Journal 89, p. 347.
[2] Jeffrey Reiman (1995), "Conduciendo al panóptico: una exploración filosófica de los riesgos a la privacidad planteados por la tecnología de la información del futuro", Santa Clara High Technology Law Journal, 11:1, p. 42.
[3] George Orwell (2008), Mil novecientos ochenta y cuatro (Londres: Penguin), págs. 4-5.
[4] Daniel Solove (2008), Comprensión de la privacidad (Cambridge, MA: Harvard University Press), pág. 98.

propensos a postularse para un cargo público. El efecto agregado de inhibiciones a menudo meramente marginales puede sofocar lo que una vez fue una sociedad libre, especialmente cuando la gente crece en un ambiente de creciente conformismo y cobardía moral. El juez del Tribunal Supremo de EEUU William O. Douglas, escribiendo su voto particular en el asunto *Osborn c. Estados Unidos*, describe de forma impresionante de la siguiente manera la amenaza que la vigilancia masiva plantea a nuestras libertades democráticas:

> "... Puede llegar el momento en que nadie pueda estar seguro de si sus palabras están siendo registradas para su uso en algún momento futuro; cuando todos temerán que sus más secretos pensamientos ya no son suyos, sino del Gobierno; cuando las conversaciones más confidenciales e íntimas siempre estén abiertas a oídos ansiosos e indiscretos. Cuando llegue ese momento, la privacidad, y con ella la libertad, se habrán ido. Si la privacidad de un hombre puede ser invadida a voluntad, ¿quién puede decir que es libre? Si cada una de sus palabras es anotada y evaluada, o si tiene miedo de que cada palabra pueda serlo, ¿quién puede decir que disfruta de la libertad de hablar? Si todas sus asociaciones son conocidas y registradas, si las conversaciones con sus asociados son sustraídas, ¿quién puede decir que goza de libertad de asociación? cuando tales condiciones se den, nuestros ciudadanos tendrán miedo de pronunciar cualquier cosa que no sea la más segura y los pensamientos más ortodoxos; temeroso de asociarse con cualquiera excepto con las personas más aceptables. La libertad tal como la contempla la Constitución habrá desaparecido."[5]

9. Para concluir, el desarrollo de nuevas tecnologías que permiten la vigilancia y un uso más eficaz de la información recopilada implica mayores amenazas a la privacidad, así como el riesgo de abuso en relación con los datos personales. No es nuestra intención afirmar que estas amenazas y riesgos ya se han materializado a gran escala o han producido las consecuencias discutidas anteriormente. Sin embargo, uno debe ser debidamente consciente de su existencia a la hora de diseñar un sistema capaz de prevenir, detectar y sancionar cualquier abuso que pueda ocurrir.

10. En nuestra opinión, estas consideraciones deberían haber llevado al Tribunal a dar mucho más peso a la vida privada en general, y a la confidencialidad de la correspondencia en particular, a ponderarla en el equilibrio contra los intereses legítimos del Estado demandado en operar su sistema de interceptación masiva. En consecuencia, la Gran Sala debería haber (a) identificado con precisión y otorgado el peso adecuado a las interferencias con la vida privada y la correspondencia; (b) haber introducido unas salvaguardas mínimas claras capaces de proteger a las personas contra los actos de interferencia arbitrarios o excesivos; y en consecuencia (c) evaluar el sistema de interceptación masiva impugnada de una manera más estricta.

II. INTERFERENCIAS EN LA VIDA PRIVADA Y LA CORRESPONDENCIA

11. En el párrafo 325 de la sentencia, la mayoría describe las etapas del sistema de intercepción masiva. Consideran que la etapa inicial, descrita como la interceptación y retención inicial de comunicaciones y datos relacionados con las comunicaciones, seguida del descarte inmediato de partes de las comunicaciones, "no constituye una injerencia especialmente significativa" (párrafo 330 de la sentencia). Respetuosamente discrepamos. Nuestra creencia es que ya en esta etapa, la interferencia es significativa. Primero, mediante la intercepción y retención inicial, todas las comunicaciones de cualquier individuo que fluyan a través de portadores seleccionados y todos los datos relacionados con las comunicaciones llegan a manos de las autoridades estatales. En segundo lugar, si bien es cierto que en esta etapa el contenido de esas comunicaciones

[5] *Osborn c. Estados Unidos*, 385 U.S. 323 (1966).

aún no ha sido analizado o señalado para la atención de los que toman decisiones y, por lo tanto, aún no puede llevar a que se tome ninguna acción contra un individuo en particular, la primera etapa es una condición *sine qua non* para cualquier etapa posterior. El alcance exacto de las comunicaciones y los datos relacionados así recopilados por los servicios de inteligencia es desconocido. Pero hay razones para creer que, de forma regular, gran parte de las comunicaciones son interceptadas. Esta situación es agravada por el hecho de que, por regla general, las personas afectadas no serán conscientes de esta interferencia. En tal situación, cuando las personas no pueden saber si sus comunicaciones están siendo dirigidas, pero son conscientes de que existe una alta probabilidad de que esto esté sucediendo, surge un tercer elemento de interferencia: las personas pueden adaptar su comportamiento, con muchas consecuencias, como se describe anteriormente en los párrafos 3 a 8 de este voto particular.

12. Según el párrafo 330 de la Sentencia, parte de las comunicaciones interceptadas se descartan inmediatamente. El Tribunal no ha sido informado sobre cómo se realiza este "descarte". Puede asumirse razonablemente que no se lleva a cabo al azar sin ningún tipo de procedimiento lógico y que en este ejercicio los servicios de inteligencia aplican ciertos criterios que separan el material basura del potencialmente útil. El propio hecho de que este acto se realice en la oscuridad y sobre una base desconocida debe, en nuestra opinión, ser motivo de grave preocupación. Tal falta de transparencia, difícilmente puede cumplir con el requisito de previsibilidad, siendo éste a su vez una de las condiciones previas para la legalidad de cualquier interferencia en los derechos protegidos por el artículo 8 del Convenio. Sin embargo, la mayoría falla al evaluar este paso en particular en el proceso de interceptación masiva de cualquier manera. Consideremos esta cuestión como una deficiencia importante de la sentencia.

III. SALVAGUARDAS MÍNIMAS QUE PROTEGEN A LAS PERSONAS CONTRA LA INTERFERENCIA ARBITRARIA O EXCESIVA.

13. En el párrafo 335, la sentencia describe la jurisprudencia del Tribunal sobre los seis requisitos mínimos que deben establecerse en la legislación nacional para evitar los abusos de poder en los casos de interceptación de comunicaciones para fines de investigación criminal. Explica además que, en el asunto *Roman Zakharov contra Rusia* ([GC], núm. 47143/06, TEDH 2015), el Tribunal sostuvo que las mismas seis salvaguardas mínimas también se aplicaban en los casos en que la interceptación se realizaba por razones de seguridad nacional. En el siguiente paso, la Gran Sala identifica la necesidad de desarrollar y adaptar estos requisitos a las especificidades de la interceptación masiva y, finalmente, describe una lista de los ocho criterios que el marco legal interno debe definir claramente para dar cumplimiento al artículo 8 del Convenio (párrafo 361 de la sentencia).

14. Esa lista está muy bien respaldada por argumentos y ciertamente puede servir como protección contra la arbitrariedad y el abuso. Sin embargo, los criterios que se incluyeron en esta lista:

> (a) no sirven claramente como estándares mínimos autónomos, ya que cualquier falta del cumplimiento de cualquiera de esos estándares parece ser "reparable" en el proceso de evaluación global;
>
> (b) requieren una definición clara de salvaguardas particulares en la legislación nacional, pero no establecen ninguna protección mínima por ellos mismos; y

(c) no prevén ninguna protección sustantiva clara de un individuo contra las interferencias desproporcionadas, en particular en la fase de aplicación de selectores fuertes para recopilar el material, y la protección procesal proporcionada por estos criterios también es insuficiente.

15. En cuanto al apartado (a), quisiéramos dirigir la atención del lector al párrafo 360 de la sentencia, que anuncia la necesidad de una evaluación global de un régimen particular de interceptación masiva. Si bien esto puede parecer atractivo, erosiona necesariamente la importancia de cada salvaguarda. Por el contrario, consideramos que cada salvaguarda etiquetada como mínima nunca puede compensarse por cualquier factor de contrapeso proporcionado con respecto a algún otro criterio. En otras palabras, el incumplimiento de una salvaguarda que se considera mínima debería conducir automáticamente a la constatación de una infracción del artículo 8 del Convenio, independientemente de si una evaluación global pudiera revelar una imagen más positiva. Lamentablemente, la mayoría no parece haber optado por este enfoque. Añadiríamos que un enfoque que estableciera estándares mínimos como límites absolutos, como gruesas líneas rojas que no pueden ser cruzadas, proporcionaría una protección más estricta y previsible, lo que es de suma importancia en un campo donde la acción de las autoridades del Estado se llevan a cabo con un alto nivel de secreto, por lo que, en palabras de la presente sentencia (véase el párrafo 322), poca o ninguna información sobre el funcionamiento del régimen está disponible y la información disponible se expresa en una terminología oscura.

16. Con respecto al apartado (b), la mayoría afirma que los ocho criterios descritos en el párrafo 361 deben definirse claramente en el marco jurídico nacional. Si bien este es un requisito que debe ser bienvenido, en particular desde el punto de vista de la previsibilidad de la ley, estos criterios en sí mismos no establecen requisitos mínimos en materia de fondo o las condiciones de procedimiento que deben cumplirse para que pueda operar el régimen de interceptación masiva y pasar de su etapa inicial a la más intrusiva. Este defecto se remedia en parte por el hecho de que algunos (pero no todos) los elementos discutidos en los párrafos 348 a 360 de la sentencia se establecen no solo en pasajes descriptivos que hacen referencia a la jurisprudencia existente, sino también en la redacción prescriptiva que establece ciertos requisitos, particularmente respecto de la autorización de interceptación masiva en sus etapas específicas. Sin embargo, sostenemos que los requisitos que marca la mayoría no son ni de lejos suficientes para proteger a una persona contra interferencias arbitrarias, excesivas o abusivas en su vida privada y correspondencia.

17. Esto nos lleva a nuestro punto (c). En el contexto de los objetivos de interceptación, principalmente usada con el fin de detectar e investigar la actividad criminal, el Tribunal se ha referido a determinadas salvaguardas sustantivas contra el abuso. Así, el Tribunal ha requerido que la naturaleza de los delitos que pueden dar lugar a una orden de interceptación sea definida junto con las categorías de personas que pueden ver sus comunicaciones interceptadas. Además, en numerosas ocasiones el Tribunal ha recurrido al requisito de sospecha razonable. La mayoría simplemente considera que estas salvaguardas no son fácilmente aplicables en la interceptación masiva. Mientras que nosotros podemos estar de acuerdo en que no pueden ser directamente transpuestas, sigue siendo necesario desarrollar una protección sustantiva sólida, mediante la cual las salvaguardas desarrolladas en el marco de la interceptación dirigida con el fin de la

lucha contra el crimen pueden servir como una excelente fuente de inspiración, como trataremos de explicar a continuación.

18. En primer lugar, a diferencia de la interceptación selectiva para la prevención de delitos, la interceptación masiva se utiliza en gran medida con fines de seguridad nacional. Es difícil ver por qué no se debe esperar que la legislación nacional defina claramente las posibles amenazas a la seguridad nacional y las circunstancias en las que las amenazas pueden desencadenar una interceptación masiva.

19. Con respecto al segundo requisito sustantivo requerido para la interceptación, es decir, la definición de las categorías de personas que pueden ver sus comunicaciones interceptadas, puede reconocerse que un requisito similar tendría poco sentido en la primera etapa de la interceptación masiva, cuando todas las comunicaciones que atraviesan ciertos portadores son interceptadas indiscriminadamente. Sin embargo, la amplitud de la interferencia no debería ser una excusa para abandonar una salvaguarda particular. Además, en etapas posteriores de la interceptación masiva, particularmente cuando se aplican selectores fuertes con el fin de señalar y analizar las comunicaciones de un individuo, la situación se vuelve en gran medida comparable a la de la interceptación dirigida. Esperamos que el marco legal defina las categorías de personas a las que se puede dirigir la aplicación de selectores fuertes por no ser un requisito excesivo, sino más bien totalmente apropiado.

20. En tercer lugar, el requisito de sospecha razonable supone una importante protección contra interferencias arbitrarias y desproporcionadas de varios derechos del Convenio. Se refiere a la probabilidad de que un delito que dé lugar a una interferencia se haya cometido o está a punto de cometerse. Si bien la interceptación masiva no debe utilizarse en la investigación de delitos, sino más bien limitarse a fines de seguridad nacional, creemos que un estándar similar a la sospecha razonable debe establecerse en relación con los motivos por los que se puede autorizar la interceptación masiva. Esto es particularmente pertinente cuando la intercepción comienza a apuntar a una persona identificada a través de la aplicación de selectores fuertes. Siendo claros, consideramos que en una sociedad democrática los servicios de inteligencia solo pueden inspeccionar las comunicaciones y los datos de comunicaciones de un individuo una vez que puedan demostrar a un observador objetivo que ese individuo puede estar comprometido o está a punto de participar en actividades que infrinjan un interés de seguridad nacional específico, o es una persona que está o puede estar en contacto con personas involucradas o a punto de participar en tales actividades. No se ha introducido tal requisito ni ninguno similar por la mayoría en la presente sentencia.

21. En lugar de estas tres salvaguardas, la mayoría ha establecido un requisito sustantivo amplio, a saber, que los motivos por los que la interceptación masiva puede ser autorizada y las circunstancias en las que las comunicaciones individuales pueden ser interceptadas deben estar claramente definidos en el marco legal interno. Desafortunadamente, la referencia a “motivos” y “circunstancias” es bastante vaga, particularmente en ausencia de cualquier referencia a cuáles pueden ser o no tales motivos y circunstancias. Además, según el lenguaje utilizado en el párrafo 361 de la sentencia, el requisito específico relativo a los motivos solo se aplica a la etapa de autorización de la interceptación masiva y no a ninguna etapa más, por lo que no da ninguna indicación sobre si el requisito se aplica, por ejemplo, a la aplicación de selectores fuertes dirigidos a las comunicaciones de una persona identificada.

22. La falta de una protección sustantiva adecuada influye en la eficacia de la protección procesal. El elemento principal de la protección procesal es el requisito de autorización previa, que la presente sentencia introduce tanto en la primera etapa de la interceptación masiva como antes de la aplicación de los selectores fuertes. El punto crucial de cualquier autorización previa es verificar si la interferencia prevista cumple con los criterios sustantivos para tal interferencia. Sin embargo, si los criterios sustantivos son vagos, demasiado amplios o incluso inexistentes, el requisito de la autorización previa no proporcionará necesariamente una protección eficaz y suficiente frente la arbitrariedad y el abuso.

23. Con respecto al requisito de autorización previa, la sentencia requiere que dicha autorización sea llevada a cabo en la etapa inicial por un organismo que sea independiente del ejecutivo. Podemos estar de acuerdo. Sin embargo, respetuosamente, estamos en total desacuerdo con que sea suficiente que la aplicación de selectores fuertes relativos a personas identificables estén sujetos solo a una previa autorización interna. En cambio, consideramos que, en esta etapa, sería necesario el control judicial previo. Si bien la jurisprudencia existente del Tribunal no necesariamente requiere autorización judicial para la interceptación selectiva de comunicaciones de individuos, entendemos que existen razones para aplicar un estándar reforzado de protección en casos de aplicación de selectores fuertes en la interceptación masiva. Estas razones son las siguientes:

> (a) La interceptación masiva, a diferencia de la intercepción dirigida, no está limitada a una categoría específica de personas y, por lo tanto, es susceptible de ser examinado un grupo mucho mayor de comunicaciones que en el caso de comunicaciones dirigidas.
>
> (b) Además, un selector fuerte perteneciente a un individuo identificado puede, cuando se aplica, abrir la puerta a un número mucho mayor de comunicaciones, esto es, a cualesquiera en las que se haga referencia a ese individuo específico, incluso si él o ella no está involucrado en esas comunicaciones (a diferencia de una comunicación "sobre", una comunicación implica que él o ella personalmente participan).
>
> (c) En la interceptación selectiva para los fines previstos en la ley, algún mecanismo de control judicial generalmente se dará en algún momento. Por ejemplo, cuando la evidencia se obtiene mediante la interceptación dirigida, será presentada en procedimientos penales posteriores, de modo que el tribunal que resuelva esos procedimientos podrá verificar si la interceptación dirigida en ese caso cumplió con los requisitos legales. Tal control judicial *a posteriori* no ocurrirá normalmente en los casos de interceptación masiva en los que se ha producido la aplicación de selectores fuertes.

24. En marcado contraste con este punto de vista, la mayoría considera que la previa autorización interna es suficiente. En nuestra opinión, la autorización interna no puede proporcionar un nivel de protección contra la arbitrariedad y el abuso comparable a la protección que ofrece el escrutinio independiente. En particular, es difícil imaginar cómo una persona que pertenece a una organización y, posiblemente, tiene conexión con la autoridad requirente podría evaluar adecuadamente una solicitud de manera justa y desinteresada. Es probable que los requisitos de la autorización no se respetaran plenamente y, por lo tanto, que el fin mismo de esta salvaguarda no se cumpliera. Esto

es incluso más probable en aquellas Partes Contratantes donde no existe una larga tradición democrática ni existe supervisión de los servicios de inteligencia.

25. Observamos que los Gobiernos del Reino Unido y los Países Bajos han alegado que cualquier requisito relativo a explicar o fundamentar los selectores o los criterios de búsqueda restringirían seriamente la eficacia de la interceptación (párrafo 353 de la sentencia) y que la mayoría demuestra cierta simpatía por este argumento (apartado 354 de la sentencia). Nosotros no podemos suscribir este argumento. Consideramos que, en una sociedad democrática, las comunicaciones y los datos relacionados con las comunicaciones de un individuo no pueden ser identificados y examinados sin su consentimiento a menos que existan razones muy convincentes para hacerlo. Si un servicio de inteligencia u otra autoridad no es capaz de articular tales razones y demostrarlas ante una institución independiente, esto debería simplemente significar que no debería tener ningún acceso a dichas comunicaciones. Reconocemos que ocasionalmente puede surgir una situación en la que el proceso de autorización sea demasiado engorroso para neutralizar eficazmente una amenaza para la seguridad nacional, y que deben proporcionarse otras soluciones al respecto. Sin embargo, si un sólido sistema de autorización diseñado para proteger adecuadamente los derechos humanos se percibe como un obstáculo innecesario, la sociedad democrática debe ser puesta en aviso.

IV. EVALUACIÓN DEL RÉGIMEN DE INTERCEPCIÓN MASIVA EN CUESTIÓN.

26. Coincidimos con los demás miembros de la Gran Sala en sus conclusiones de los puntos 1, 2 y 4 de la parte dispositiva de la sentencia. Dicho eso creemos que la evaluación de ciertas características del régimen impugnado no va lo suficientemente lejos y no se identifican correctamente algunos de sus defectos.

27. Como ejemplo, deseamos dirigir la atención del lector a los motivos por los que se podía autorizar la interceptación masiva bajo el sistema del Reino Unido (apartados 368 a 371 de la sentencia). Podía emitirse una orden de interceptación masiva si fuera necesario (a) en interés de la seguridad nacional; (b) con el fin de prevenir o detectar delitos graves; o (c) con el fin de salvaguardar el bienestar económico de del Reino Unido en la medida en que esos intereses también fueran relevantes para los intereses de seguridad nacional.

28. Ambos fines (a) y (c) hacen referencia a intereses de seguridad nacional. Parece que ni la seguridad nacional ni sus intereses estaban definidos en ningún lugar. Si bien tomamos nota de la referencia de la sentencia a la aclaración del Comisionado IC sobre cómo en la práctica se percibía el término “seguridad nacional” (párrafo 369 de la sentencia), sostenemos que esta aclaración sigue siendo insuficiente desde el punto de vista del requisito de previsibilidad. Además, tenemos dudas sobre si la aclaración del Comisionado IC puede asimilarse a una jurisprudencia que, según la jurisprudencia del Tribunal, pueda compensar la vaguedad en la legislación. Como consecuencia de la ausencia de una definición clara, un individuo no puede estar seguro, incluso contando con asesoramiento, sobre por qué motivos exactos sus comunicaciones podrían ser interceptadas y analizadas por los servicios de inteligencia.

29. El fin (b) no tenía el fallo antes mencionado en los fines (a) y (c). El delito grave se definió como un delito por que el autor (suponiendo que tuviera más de veintiún años y no tuviera condenas previas) podía esperar razonablemente ser condenado a una pena de prisión de tres años o más, o cuando se llevara a cabo una conducta que implicara el uso

de la violencia, resultara en una ganancia financiera sustancial o fuera realizada por un gran número de personas en la búsqueda de un fin común (ver párrafo 369 de la sentencia). Tal definición cubre un muy amplio ámbito de conductas, lo que plantea serias dudas sobre la proporcionalidad de este motivo. Además, en una sociedad democrática, los servicios de inteligencia no deben tener ninguna competencia en la lucha contra la delincuencia, a menos que las actividades delictivas amenacen la seguridad nacional[6]. La explicación del Gobierno demandado, de que la información obtenida mediante interceptación masiva no se podía utilizar en el enjuiciamiento de un delito penal, es en nuestra opinión poco convincente. Parece que, sobre la base de la información así obtenida, los organismos encargados de hacer cumplir la ley podían actuar, por ejemplo, procediendo a llevar a cabo medidas de investigación o incluso detenciones, lo que a su vez produciría pruebas con el fin de enjuiciar. Es probable que, en un futuro no tan lejano, al explorar este terreno en particular, la investigación del crimen pudiera pasar de la vigilancia dirigida a la interceptación masiva de datos.

V. CONCLUSIÓN

30. Son escasas las ocasiones en las que el Tribunal se pronuncia sobre un caso que afecta al futuro de nuestras sociedades. El presente caso es un ejemplo. La Gran Sala ha aprovechado en parte la oportunidad y ha esbozado un conjunto integral de principios que tienen como objetivo proteger los derechos humanos y libertades fundamentales, en particular los consagrados en los artículos 8 y 10 del Convenio. Sin embargo, por las razones explicadas en este voto particular, al realizar el ejercicio de equilibrio, la mayoría no ha asignado el peso adecuado a la vida privada y la correspondencia, que en varios aspectos permanecen insuficientemente protegidos frente a la interceptación masiva de comunicaciones. Cabe esperar que en casos futuros que planteen cuestiones sobre interferencias concretas con los derechos de individuos específicos, el Tribunal interpretará y desarrollará aún más los principios de una manera que defienda adecuadamente a la sociedad democrática y los valores que defiende.

[6] Véase, por ejemplo, la Recomendación 1402 (1999) de la Asamblea Parlamentaria del Consejo de Europa sobre el control de los servicios de seguridad interior en los Estados Miembros del Consejo de Europa, en particular, la Directriz A (ii). Esta Recomendación aborda las actividades de los servicios de seguridad internos, pero la consideramos perfectamente aplicable también a la inteligencia extranjera.

VOTO PARTICULAR PARCIALMENTE CONCURRENTE Y PARCIALMENTE DISIDENTE DEL JUEZ PINTO DE ALBUQUERQUE

I. Introducción (§ 1)

II. Deconstrucción del régimen de intercepción masiva *pro autoritae* del Tribunal (§§ 2-18)

A. Lenguaje vago (§ 2-3)

B. Metodología sesgada (§§ 4-12)

C. Régimen de salvaguardas defectuoso (§§ 13-15)

D. Conclusión preliminar (§§ 16-18)

III. Construcción de un régimen de interceptación masiva *pro persona* (§§ 19-34)

A. Interceptación masiva de comunicaciones (§§ 19-29)

B. Intercambio de datos interceptados con servicios de inteligencia extranjeros (§§ 30-31)

C. Interceptación masiva de datos relacionados con las comunicaciones (§ 32)

D. Conclusión preliminar (§§ 33-34)

IV. Crítica sobre el régimen de interceptación masiva del Reino Unido impugnado (§§ 35-58)

A. Interceptación masiva de comunicaciones bajo la RIPA (§§ 35-49)

B. Intercambio de datos interceptados con servicios de inteligencia extranjeros bajo el Capítulo 12 del Código IC (§§ 50-54)

C. Interceptación masiva de datos relacionados con las comunicaciones en el marco de la RIPA (§§ 55-57)

D. Conclusión preliminar (§ 58)

V. Conclusión (§§ 59-60)

I. INTRODUCCIÓN

1. Voté con la mayoría, excepto en relación a la no violación de los artículos 8 y 10 en relación con la recepción de material interceptado por los servicios de inteligencia extranjeros, a saber, el material interceptado de forma masiva por la Agencia de Seguridad Nacional de los Estados Unidos ("NSA"- siglas en inglés-) a través de los programas PRISM y UPSTREAM. Asimismo, no estoy de acuerdo con el núcleo del

razonamiento mayoritario con respecto a la constatación de una violación de los artículos 8 y 10. El fin de esta opinión es exponer las razones de mi desacuerdo[1].

II. DECONSTRUCCIÓN DEL RÉGIMEN DE INTERCEPCIÓN MASIVA *PRO AUTORITAE* DEL TRIBUNAL

A. Lenguaje vago

2. Lamento decir desde el principio que el lenguaje del Tribunal es inadmisiblemente vago, como se demostrará en este dictamen. Mientras a veces este lenguaje refleja la intención deliberada del Tribunal de otorgar margen para la ejecución discrecional de esta sentencia por parte del Estado demandado, en otras ocasiones muestra la vacilación de los jueces en la ejecución de su función jurisdiccional. Al hacerlo, no sólo debilitan el poder del Tribunal, sino que diluyen el valor normativo de esta sentencia.

3. Dado que los conceptos jurídicos del derecho europeo de los Derechos Humanos son autónomos, en el sentido de que no dependen estrictamente del significado y alcance de los correspondientes conceptos jurídicos en el derecho interno, y dado el carácter novedoso de las cuestiones jurídicas en juego ante la Gran Sala, el Tribunal debió haber establecido, de forma clara, el significado de los conceptos jurídicos fundamentales que utiliza en la presente sentencia[2], independientemente de su significado en la Ley de Regulación de los Poderes de Investigación 2000 (RIPA), el Código de prácticas de interceptación de comunicaciones (Código IC) o cualquier disposición "por debajo de la línea de flotación". Por motivos de claridad, utilizaré los términos enumerados a continuación con los siguientes significados:

> (a) "**sujeto de la interceptación**" abarca a las personas físicas y jurídicas, incluyendo servicios públicos, corporaciones privadas, ONGs y cualquier organización de la sociedad civil, cuyas comunicaciones electrónicas puedan ser interceptadas o hayan sido interceptadas[3];
>
> (b) "**material interceptado**" o "**material masivo**" comprende el contenido de las comunicaciones electrónicas y los datos de dichas comunicaciones que se han recopilado mediante interceptación masiva[4];
>
> (c) "**datos relacionados con las comunicaciones**" incluye los datos necesarios para localizar a la fuente de una comunicación electrónica y su destino, para determinar la fecha, tiempo, duración y tipo de comunicación, para la identificación de los equipos de comunicaciones utilizados, y para localizar el equipo terminal y las comunicaciones, datos que comprenden, entre otros, el nombre y la dirección del usuario, los números de teléfono de la persona que llama y de la persona que recibe la llamada, y la dirección IP respecto a los servicios de Internet[5];

[1] Esta es la segunda vez que escribo un voto particular sobre la interceptación masiva. En *Szábo y Vissy contra Hungría*, núm. 37138/14, 12 de enero de 2016, tuve la oportunidad de manifestar mi punto de vista sobre la pendiente resbaladiza en la que el régimen húngaro de interceptación masiva se había convertido y las consecuencias indeseables que acechan al pie de la pendiente. En vista del debate mantenido en la Gran Sala, y después de sopesar cuidadosamente todos los argumentos en conflicto, ahora puedo afirmar que no me he movido ni un centímetro de mi posición anterior. De hecho, ahora estoy aún más convencido de que lo que escribí en 2016, lamentablemente, sigue estando muy actualizado. Por lo tanto, el presente voto particular debe leerse junto con lo que escribí hace cinco años.

[2] Esta buena práctica se puede encontrar, por ejemplo, en *Rohlena c. La República Checa* [GC], núm. 59552/08, 27 de enero de 2015.

[3] El concepto interno es similar. Consulte la sección 20 de la RIPA.

[4] El concepto interno es diferente. Consulte la sección 20 de la RIPA

[5] El concepto interno es más limitado. Consulte la sección 20 de la RIPA. La sección 21 (4), (6) y (7) establece el concepto de "datos de las comunicaciones".

(d) "**interceptación masiva**" como interceptación dirigida y no dirigida de comunicaciones (y datos relacionados con las comunicaciones) que circulan en portadores por medio de selectores fuertes y selectores;

(e) "**portadores**" como transportadores (principalmente cables submarinos de fibra óptica) de comunicaciones;

(f) "**selectores fuertes**" como identificadores (personales) específicos relacionados con una persona identificada o un objetivo identificable, que permiten la adquisición de comunicaciones electrónicas a, desde, o sobre el objetivo;

(g) "**selectores**" como identificadores no específicos (no personales);

(h) **una comunicación "a" o "desde"** como una comunicación electrónica en la cual el remitente o el destinatario es un usuario del selector asignado;

(i) **una comunicación "sobre"** como aquélla en la que se hace referencia al selector asignado dentro de la comunicación electrónica adquirida, pero el objetivo no es necesariamente un participante en la comunicación;

(j) "**comunicación externa**" como comunicación enviada o recibida fuera del territorio nacional[6];

(k) "**comunicación**" como "cualquier manifestación que comprenda habla, música, sonidos, imágenes o datos de cualquier descripción y señales que sirvan para compartir cualquier información entre personas, entre una persona y una cosa o entre cosas, o para el accionamiento o control de cualquier aparato"[7];

(l) "**disposiciones por debajo de la línea de flotación**" como reglas y prácticas internas secretas de la autoridad interceptora.

B. Metodología sesgada

4. Es lamentable el enfoque metodológico del Tribunal en este caso, por dos razones principales. Primero, el Tribunal estaba dispuesto a decidir un caso de esta importancia "sobre la base de información limitada sobre la forma en que esos regímenes [de interceptación masiva de los Estados contratantes] funcionan"[8]. Por ejemplo, el Gobierno no indicó el número ni 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 relacionados con comunicaciones y, sin embargo, el Tribunal no insistió en obtener esa información crucial. El Tribunal de Poderes de Investigación (IPT) examinó las disposiciones "por debajo de la línea de flotación"[9], el Comisionado de Interceptación de Comunicaciones (Comisionado IC) tuvo acceso al "material cerrado"[10] e incluso el Revisor Independiente de la Legislación sobre Terrorismo examinó "una gran cantidad de material cerrado"[11], pero el Tribunal no lo hizo y no pudo hacerlo. El Tribunal evidentemente carecía del material detallado necesario para hacer un análisis estructural completo y evaluar la interceptación masiva en el Reino Unido. Es decepcionante que la extrema sensibilidad del tema de esta sentencia, que fue reiteradamente subrayada por el Tribunal, sólo sirviera a fin de insistir en la necesidad

[6] Este concepto es similar al del artículo 20 de la RIPA.
[7] Este concepto está consagrado en el artículo 81 de la RIPA, que también puede ser tenido en cuenta por el Tribunal.
[8] Párrafo 323 de la presente Sentencia.
[9] Párrafos 33 y 50 de la presente Sentencia.
[10] Párrafo 136 de la presente Sentencia.
[11] Párrafo 424 de la presente Sentencia.

de la "eficacia"[12] y la "flexibilidad"[13] del sistema de interceptación masiva, pero no para recopilar todas las pruebas necesarias para que la sentencia del Tribunal fuera objetivamente sólida. Esta autoimpuesta restricción de la facultad del Tribunal para recabar pruebas demuestra que los jueces de Estrasburgo no consideran al Tribunal como un verdadero órgano judicial, con la facultad de ordenar a las partes que les proporcionen ilimitada e incondicionalmente acceso a las pruebas pertinentes al objeto del caso. En consecuencia, el Tribunal hizo algunas "suposiciones fundadas" 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 "suposiciones fundadas" es que refleja las hipótesis del regulador y sus sesgos. Y son claros en el presente caso. El argumento del Gobierno se reduce a una simple proposición que es "confíe en nosotros". La mayoría estaba dispuesta a aceptar esta proposición, con el riesgo de errar respecto a la recolección excesiva de inteligencia. Yo no. Como expresó la Junta de Revisión Presidencial de los Estados Unidos: "Los estadounidenses no deben cometer el error de confiar en los funcionarios"[14]. Diría lo mismo para los europeos.

5. En segundo lugar, las pruebas autoimpuestas antes mencionadas y la limitación de su jurisdicción llevan al Tribunal a asumir la inevitabilidad de la interceptación masiva y, más aún, la de una manta, no dirigida, un régimen de interceptación sin sospechas, según lo alegado por el Estado demandado y los terceros tanto en el presente caso como en el asunto *Centrum för rättvisa c. Suecia*[15]. Con un razonamiento circular, el Gobierno afirmó que la interceptación masiva era incompatible con un requisito de sospecha razonable, porque, por definición, no estaba dirigida, y no estaba dirigida porque no requería sospecha[16]. El Tribunal siguió este ejemplo y lo expresó en términos axiomáticos:

> "El requisito de "sospecha razonable", que se puede encontrar en la jurisprudencia del Tribunal sobre la interceptación selectiva en el contexto de las investigaciones penales es menos pertinente en el contexto de la interceptación masiva, cuyo fin es, en principio, preventivo, más que la investigación de un objetivo específico y / o un delito identificable "[17]

De este nuevo paradigma se desprende que el Tribunal se ha apartado de la jurisprudencia según la cual "no considera que exista fundamento para aplicar diferentes principios sobre la accesibilidad y claridad de las reglas que gobiernan la interceptación de comunicaciones individuales, por una de un lado, y los programas de vigilancia más

[12] Párrafo 353 de la presente Sentencia.
[13] Párrafo 354 de la presente Sentencia.
[14] "Libertad y seguridad en un mundo cambiante", Informe y recomendaciones del Grupo de revisión del Presidente sobre inteligencia y comunicaciones tecnológicas, 12 de diciembre de 2013, pág. 114.
[15] *Centrum för rättvisa c. Suecia* (núm. 35252/08), dictada el mismo día que la presente sentencia. Es notable que los gobiernos de Francia, los Países Bajos y Noruega se centraron precisamente en este punto: según ellos, no había ninguna justificación para añadir el requisito de sospecha razonable para la interceptación masiva (párrafos 301, 305 y 309 de esta sentencia).
[16] Véase la alegación del Gobierno demandado ante la Gran Sala el 10 de julio 2019: "Estos requisitos [sospecha razonable y notificación posterior] son fundamentalmente incompatibles con el funcionamiento de un régimen que no depende de la existencia de objetivos de vigilancia claramente definidos. El régimen de la sección 8 (4) es, por su naturaleza, un régimen que existe para descubrir amenazas de seguridad nacional desconocidas y delitos graves. Entonces una sospecha razonable simplemente no podría formar parte de él. Tal requisito paralizaría su utilidad…". Finalmente, el argumento se reduce a la "utilidad" de la sospecha razonable en la interceptación masiva.
[17] Párrafo 348 de la presente Sentencia.

generales, por otro"[18] Los sistemas de interceptación masiva alemán y británico ya habían sido evaluados por el Tribunal bajo exactamente los mismos criterios aplicables a la interceptación dirigida: me refiero a la vigilancia estratégica generalizada bajo la Ley G10 en *Weber y Saravia c. Alemania*[19], así como la recopilación indiscriminada de telecomunicaciones enviadas o recibidas fuera de las Islas Británicas bajo la Ley de Interceptación de Comunicaciones de 1985 en *Liberty y Otros contra el Reino Unido*[20] y la captura de grandes cantidades de comunicaciones en virtud de la Ley de Regulación de Poderes de Investigación de 2000 en *Kennedy contra el Reino Unido*[21]. El Tribunal se ha apartado de los fundamentos de esta jurisprudencia sin una buena razón, como demostraré más abajo.

6. Además, el Tribunal no dio la debida importancia al hecho de que había reformulado y aplicado de forma efectiva la jurisprudencia anterior en tres casos recientes cuyo fondo incluía, en un caso tangencialmente y en los otros dos específicamente, la interceptación de comunicaciones no dirigida. Me refiero a los asuntos *Roman Zakharov contra Rusia* [22], *Szábo y Vissy contra Hungría*[23] y *Mustafa Sezgin Tanrıkulu contra Turquía*[24]. Es revelador que en el asunto *Roman Zakharov contra Rusia*[25] también utilizó los criterios de *Weber y Saravia* cuando se trataba de llevar a cabo actividades de búsqueda, incluyendo la interferencia de correos, telégrafos y otras comunicaciones, lo que podía afectar a "cualquier persona que utilice estos servicios telefónicos"[26], para fines de seguridad nacional, militar, económicos o ecológicos[27]. La Gran Sala en ese caso fue tan lejos como para reprochar la práctica de las "autorizaciones de interceptación que no mencionan a una persona específica o el número de teléfono que va ser intervenido y autorizan la intercepción de todas las comunicaciones telefónicas en el área donde se ha cometido un delito"[28]. En *Szábo y Vissy c. Hungría*[29], el Tribunal fue incluso más explícito al censurar la "vigilancia ilimitada de un gran número de ciudadanos"[30], a los efectos de la lucha contra el terrorismo y el rescate de ciudadanos húngaros en peligro en el extranjero[31]. Si bien admite la necesidad de una intercepción masiva para contrarrestar las amenazas internas y externas, el Tribunal requería que existiera una "sospecha individual"[32] para toda medida de vigilancia a la luz de los criterios de *Weber y Saravia*[33]. En el caso posterior *Mustafa Sezgin Tanrıkulu contra Turquía*[34], el Tribunal reprochó la decisión del tribunal interno de permitir la interceptación de las comunicaciones telefónicas y

[18] *Liberty y otros contra el Reino Unido*, núm. 58243/00, § 63, 1 de julio de 2008.
[19] *Weber y Saravia contra Alemania* (dec.), núm. 54934/00, §§ 95 y 114, TEDH 2006 - XI.
[20] *Liberty y otros*, citada anteriormente, §§ 63-65.
[21] *Kennedy contra Reino Unido*, núm. 26839/05, §§ 158-60, 18 de mayo de 2010.
[22] *Roman Zakharov c. Rusia* [GC], núm. 47143/06, §§ 231 y 264, TEDH 2015.
[23] *Szábo y Vissy*, antes citada.
[24] *Mustafa Sezgin Tanrıkulu c. Turquía*, núm. 27473/06, 18 de julio de 2017.
[25] *Roman Zakharov*, antes citada, §§ 231 y 264.
[26] Ibíd., §§ 175-178.
[27] Ibíd., §§ 31, 246-248.
[28] Ibíd., § 265. Los casos de autorización de "vigilancia del área" claramente implicaban una potencial vigilancia masiva.
[29] *Szábo y Vissy*, citadas anteriormente.
[30] Ibíd., párr. 67.
[31] Ibíd., párr. 63.
[32] Ibíd., párr. 71
[33] Ibíd., párr. 56.
[34] *Mustafa Sezgin Tanrıkulu*, citada anteriormente, §§ 56 y 57.

electrónicas de cualquier persona en Turquía con el fin de prevenir actos delictivos de organizaciones terroristas, después de haber recordado y confirmado la jurisprudencia de *Weber y Saravia, Roman Zakharov* y *Szábo y Vissy*.

7. Además de la pretensión de que "ambos casos [*Liberty y Otros y Weber y Saravia*] ya tienen más de diez años", y que la actividad de vigilancia considerada en esos casos era "mucho más estrecha"[35], el Tribunal dio tres razones para abandonar la jurisprudencia anterior[36], del todo poco sólidas.

8. El primer argumento es que el "fin declarado" de la interceptación masiva es "en muchos casos" monitorear las comunicaciones de personas fuera de la jurisdicción territorial del Estado "que no podrían ser supervisadas mediante otras formas de vigilancia"[37]. El Tribunal no proporcionó, ni podía proporcionar, ninguna prueba de que "en muchos casos" la intercepción masiva fuera limitada, en términos de "finalidad declarada", menos aún de práctica real, a personas ajenas a la jurisdicción territorial del Estado. Por el contrario, todos los documentos de las autoridades disponibles sobre la interceptación masiva, que el Tribunal optó por ignorar, le cuentan una historia diferente. Es incomprensible que, ante la falta de pruebas proporcionada por el Gobierno demandado, el Tribunal hiciera la vista gorda ante las evaluaciones fácticas del Consejo de Europa y la Unión Europea públicamente disponibles en una plétora de documentos autorizados sobre interceptación masiva publicados después de que estallara el escándalo de Snowden, como por ejemplo las Resoluciones de la Asamblea Parlamentaria del Consejo de Europa (PACE) 1954 (2013) y 2045 (2015), y la Recomendación 2067 (2015), la Declaración del Comité de Ministros de 11 de junio de 2013 y su respuesta a la Recomendación PACE 2067 (2015), la Recomendación de la Comisión Europea contra el Racismo núm. 11, los Comentarios del Comisionado de Derechos Humanos del 24 de octubre de 2013, sus documentos temáticos de 8 de diciembre de 2014 y mayo de 2015, y su Informe sobre las deficiencias en la supervisión de los servicios de inteligencia y seguridad alemanes del 1 de octubre de 2015, las Resoluciones del Parlamento Europeo de 12 de marzo de 2014 y 29 de octubre 2015, el dictamen del Supervisor Europeo de Protección de Datos de 20 de febrero 2014, y el dictamen 4/2014 del Grupo de Trabajo del artículo 29. También descuidaron la Resolución 68/167 de la Asamblea General de las Naciones Unidas de 18 de diciembre 2013, las observaciones del Comité de Derechos Humanos de las Naciones Unidas (CDH) sobre el cuarto informe de EEUU de 26 de marzo de 2014 y la declaración conjunta del Relator Especial de Naciones Unidas y la Comisión Interamericana del Relator Especial de Derechos Humanos para la libertad de expresión de 21 de junio de 2013[38]. Lo más asombroso es que la mayoría ni siquiera consideró los documentos internacionales disponibles sobre el régimen británico de interceptación masiva, como las Observaciones finales del CDH sobre el Informe del séptimo período del Reino Unido de 17 de agosto de 2015[39], y el Memorando del Comisionado de

[35] Párrafo 341 de la presente Sentencia. Esta afirmación pasa por alto lo establecido en *Roman Zakharov y Szábo* y el asunto *Vissy*, ya mencionados.
[36] Párrafos 344-346 de la presente Sentencia.
[37] Párrafo 344 de la presente Sentencia.
[38] Para un análisis detallado de estos documentos ver mi voto particular en *Szábo y Vissy c. Hungría*, citada anteriormente.
[39] Doc. ONU CCPR/C/GBR/CO/7.

Derechos Humanos del Consejo de Europa sobre Mecanismos de vigilancia y supervisión en el Reino Unido de mayo de 2016[40].

9. Todos estos documentos, así como las recientes sentencias en los asuntos *Szábo y Vissy*[41] y *Mustafa Sezgin Tanrıkulu c. Turquía*[42] de este Tribunal y la jurisprudencia al respecto del Tribunal de Justicia de la Unión Europea (TJUE)[43], contradicen la presunta prevalencia del seguimiento de personas ajenas a la jurisdicción territorial del Estado. Por el contrario, todos ellos confirman que la vigilancia masiva está dirigida principalmente a personas dentro de la jurisdicción territorial del Estado[44]. El propio Gobierno admitió que el número de consultas de datos relacionados con comunicaciones realizadas en virtud de la sección 8 (4) de la RIPA con respecto a personas que se sabe que se encuentran en el Reino Unido: por lo tanto, como herramienta de vigilancia interna, es de varios miles por semana[45].

10. El segundo argumento que se aparta de la jurisprudencia anterior es que los Estados miembros del Consejo de Europa "parecen utilizar"[46] la interceptación masiva para fines distintos a la investigación de delitos. La línea de argumentación del Tribunal parece ser la siguiente: dado que la interceptación dirigida es empleada "en más casos"[47] que al interceptación masiva con el fin de detectar delitos y de investigación, pero la interceptación masiva también se puede utilizar con el fin de recopilar inteligencia extranjera, donde no puede haber un objetivo específico ni una infracción identificable, la interceptación masiva no es (y no debería ser) regida por los mismos estándares que la vigilancia selectiva[48]. Esto es otro argumento que todavía no ha sido probado por el Tribunal, que optó por decidir basándose en apariencias, más que en hechos.

---

[40] CommDH (2016)20.

[41] *Szábo y Vissy*, citada anteriormente, § 66: "prácticamente cualquier persona en Hungría puede ser objeto de vigilancia secreta".

[42] *Mustafa Sezgin Tanrıkulu*, citada anteriormente, §7.

[43] Párrafos 209-241 de la presente sentencia. Me refiero aquí a los casos de *Derechos Digitales Irlanda Ltd*. (sobre la Directiva de Retención de Datos 2006/24/EC que "implicó una interferencia con los derechos fundamentales de prácticamente toda la población europea"), *Maximilian Schrems* (reprochando la legislación que permite a las autoridades públicas tener acceso "de forma generalizada al contenido de las comunicaciones electrónicas"), *Privacidad Internacional* (la legislación nacional exige que los servicios de comunicación electrónica divulguen datos de tráfico y ubicación a los organismos de inteligencia mediante una transmisión general e indiscriminada que afecta a "todas las personas que utilizan servicios de comunicaciones electrónicas") y *La Quadrature du Net y Otros* (que censuran la legislación que exige que los proveedores de servicios retengan "general e indiscriminadamente" datos de tráfico y ubicación). Los dos primeros casos se referían a la tramitación de datos personales para fines previstos en la ley, los dos últimos casos a la evaluación de la vigilancia secreta realizada por los servicios de inteligencia.

[44] Véase a continuación el debate completo sobre la falta de jurisdicción territorial basada en la distinción entre comunicaciones internas y externas para justificar la interceptación masiva de estas últimas.

[45] Véanse las alegaciones del Gobierno demandado ante la Gran Sala de 2 de mayo 2019, pág. 42 ("muchos miles en una semana determinada en relación con personas que se conoce o se cree que están en el Reino Unido").

[46] Párrafo 345 de la presente Sentencia

[47] Ibíd.

[48] Cabe señalar que los Gobiernos de Francia y los Países Bajos insistieron, al igual que la Sala, que era un error suponer que la interceptación masiva constituía una intrusión mayor en la vida privada que la interceptación selectiva (párrafos 300 y 306 de esta sentencia).

11. En realidad, la interceptación masiva no dirigida está prohibida explícitamente o implícitamente en veintitrés Estados europeos[49]. Como PACE[50] y el Comisionado de Derechos Humanos del Consejo de Europa[51] han demostrado enérgicamente, la vigilancia indiscriminada de las comunicaciones ha demostrado ser ineficaz para la prevención del terrorismo y, por lo tanto, no es sólo peligrosa para la protección de los derechos humanos, sino también una pérdida de recursos. Por lo tanto, si hay un consenso en Europa sobre la interceptación masiva no dirigida, el consenso es que debería prohibirse, pero esto ha sido ignorado por el Tribunal. Solo siete Estados miembros del Consejo de Europa aplican tales regímenes[52] y lo hacen principalmente para la prevención, detección e investigación de delitos tales como terrorismo, espionaje, ciberataques y, más vagamente, "delitos graves"[53], como lo demuestran los mencionados documentos oficiales del Consejo de Europa y de la Unión Europea, las sentencias de los asuntos *Szábo y Vissy y Mustafa Sezgin Tanrıkulu* de este Tribunal y la jurisprudencia al respecto del TJUE. La recopilación de inteligencia extranjera es solo uno entre otros fines, y el Tribunal no tiene el elemento mínimo de información estadística u otra evidencia de cómo se persigue este fin, ya sea con base en el monitoreo de objetivos específicos o de otra manera. Incluso suponiendo, por el bien del debate, que la recopilación de inteligencia extranjera se lleva a cabo principalmente por medio de la interceptación masiva no dirigida, esto no implica necesariamente que toda la interceptación masiva, incluida la interceptación masiva con fines relacionados con detección e investigación de la delincuencia, deba ser no dirigida. De lo contrario, sucede que la intercepción masiva se convierte en una escapatoria para evitar las protecciones de una orden individual en circunstancias en las que dicha orden sería perfectamente adecuada para adquirir las comunicaciones en cuestión. Dicho eso, nada excluye la posibilidad de que la recopilación de inteligencia extranjera pueda llevarse a cabo mediante la interceptación masiva basada en un requisito de sospecha razonable de la participación de la persona objetivo o grupo de personas involucradas en actividades perjudiciales para la seguridad nacional, aunque no sean delitos penales[54].

12. El tercer argumento trata precisamente de esta fina línea entre intercepción dirigida a la antigua y las nuevas formas de intercepción masiva utilizadas para apuntar a individuos específicos, y es el argumento más débil del Tribunal. En el caso de la interceptación mediante selectores fuertes, el Tribunal argumenta que los "dispositivos de las personas objetivo no son monitoreados",[55] y, por lo tanto, la intercepción masiva

[49] Como concluyó el propio informe de investigación del Tribunal sobre Albania, Andorra, Austria, Bélgica, Bosnia y Herzegovina, Croacia, República Checa, Grecia, Irlanda, Islandia, Italia, Liechtenstein, Moldavia, Mónaco, Montenegro, Macedonia del Norte, Polonia, Portugal, Rumania, San Marino, Serbia, Turquía y Ucrania. Así, los párrafos 242-246 de la sentencia no reflejan una imagen correcta del panorama europeo.

[50] Resolución PACE 2031 (2015).

[51] Memorando del Comisionado de Derechos Humanos del Consejo de Europa sobre Vigilancia y Mecanismos de supervisión en el Reino Unido, CommDH (2016)20, mayo de 2016, pág. 10.

[52] Párrafo 242 de la presente Sentencia.

[53] Párrafo 345 de la presente Sentencia. Me refiero aquí a la crítica dirigida a este concepto de "delito grave" por el TJUE (ver párrafo 212 de esta sentencia).

[54] Véase el informe de la Comisión de Venecia sobre la supervisión democrática de las agencias de inteligencia de señales, 2015, pág. 9, 25 y 26 ("deben existir hechos concretos que indiquen el delito/conducta que amenaza a la seguridad, y los investigadores deben tener una "causa probable", 'sospecha razonable' o cumplir algún test similar"), y el Memorándum de Comisionado de Derechos Humanos del Consejo de Europa, citado anteriormente, p. 6.

[55] Párrafo 346 de la presente Sentencia.

no requiere las mismas garantías que la clásica interceptación dirigida. Esto no es convincente. La recogida automática y el procesamiento por medio de selectores fuertes que permitan la adquisición de comunicaciones electrónicas a, desde o sobre el objetivo a través de los portadores elegidos por los servicios de inteligencia es potencialmente una forma mucho más intrusiva de interferencia con los derechos del artículo 8 que la mera supervisión de los dispositivos de las personas objetivo[56]. Por lo tanto, es engañoso decir que "sólo" (§ 346) esos paquetes de comunicaciones de las personas objetivo serán interceptados, dando la impresión de que la intercepción masiva basada en selectores fuerte es menos intrusiva que el anticuado control de un dispositivo del individuo.

C. Régimen defectuoso de salvaguardas.

13. De este razonamiento fácticamente infundado, el Tribunal extrajo dos conclusiones sobre "el enfoque a seguir en los casos de interceptación masiva"[57]: el derecho interno no tiene que identificar la naturaleza de los delitos que pueden dan lugar a una orden de interceptación y las categorías de personas cuyas comunicaciones pueden ser interceptadas, y no se necesita el requisito de sospecha para fundamentar tal orden de interceptación[58]. De acuerdo con la lógica del Tribunal, ya que "el fin de [la interceptación masiva] es en principio preventivo, más que para la investigación de un objetivo específico y / o un delito identificable"[59], ninguna de las dos salvaguardas anteriores es requerida en la legislación nacional, incluso cuando la interceptación masiva se dirige a un individuo involucrado en un delito identificable. Así, en general, una orden de intercepción sin sospechas es suficiente para desencadenar una intercepción masiva, ya sea para fines de detección e investigación de delitos u otros.

14. La posición del Tribunal deja muchas preguntas sin respuesta. ¿Cuáles son los motivos admisibles para acudir a la interceptación masiva? Por ejemplo, ¿es la investigación de "delitos graves", sin mayor precisión, un motivo admisible? ¿Qué tan grave debe ser el delito investigado? ¿Es la investigación del robo de una cartera y un teléfono móvil admisible?[60] ¿Es la promoción del espionaje económico e industrial en aras del bienestar económico y la seguridad nacional de los interceptores un motivo admisible?[61]¿Cuáles son las "circunstancias" admisibles en las qué las comunicaciones de un individuo pueden ser interceptadas? Para justificar el volumen interceptación de las comunicaciones de un individuo, ¿cuál es el grado de interés requerido de las comunicaciones del individuo para los fines perseguidos por la orden de interceptación masiva? ¿Es aplicable el estándar de sospecha individual mencionado en *Szábo y Vissy*[62] o el criterio de sospecha razonable requerido en *Roman Zakharov*[63]? ¿Cómo puede el

[56] Como explicó el TJUE en su sentencia *Derechos Digitales Irlanda*, citada anteriormente, § 55: "la necesidad de ... salvaguardas es tanto mayor cuando ... los datos personales están sujetos a un procesamiento automático".
[57] Punto (c) (iii) de la valoración del Tribunal.
[58] Párrafo 348 de la presente Sentencia.
[59] Ibíd.
[60] El ejemplo deriva de la jurisprudencia del TJUE (véase el apartado 220 de la presente sentencia).
[61] El ejemplo deriva de la aguda crítica contenida en la Resolución del Parlamento Europeo de 12 de marzo de 2014 sobre el programa de vigilancia de la NSA de EEUU. El Informe de la Comisión de Venecia, antes citado, p. 18, y el Memorando del Comisionado de Derechos Humanos del Consejo de Europa, antes citado, pág. 8.
[62] *Szábo y Vissy*, antes citada, § 71.
[63] *Roman Zakharov*, antes citada, §§ 260, 262 y 263.

Tribunal exigir que la ley establezca "con suficiente claridad"[64] los fundamentos sobre los cuales la interceptación puede ser autorizada y las circunstancias en las que las comunicaciones de los particulares pueden ser interceptadas cuando el Tribunal no es suficientemente claro sobre a qué tipo de "fundamentos" y "circunstancias" se está refiriendo?

15. Dado que el artículo 8 se aplica a todas las etapas de la interceptación masiva, incluidas la retención inicial de comunicaciones y datos relacionados con las comunicaciones[65], el Tribunal ha establecido correctamente "salvaguardas de extremo a extremo"[66]. El problema es que el Tribunal no tiene clara la naturaleza jurídica de las "salvaguardas de extremo a extremo". Por un lado, ha utilizado un lenguaje imperativo ("debe hacerse"[67], "debe estar sujeto"[68], "debe ser autorizado"[69], "debe ser informado"[70], "debe estar justificado" [71], y "debe registrarse escrupulosamente"[72], "también debe estar sujeto"[73], "es imperativo que el recurso debe"[74]) y las ha denominado "salvaguardas fundamentales"[75] e incluso "salvaguardas mínimas"[76]. Pero, por otro lado, ha diluido estas salvaguardas en "una evaluación global del funcionamiento del régimen"[77], permitiendo una compensación entre las salvaguardas[78]. Parece que finalmente cada salvaguarda individual no es obligatoria, y el lenguaje prescriptivo del Tribunal no se corresponde realmente con las características innegociables del sistema nacional. En algunos rincones de Europa, los celosos servicios secretos se verán fuertemente tentados a aprovechar la forma tan laxa del Tribunal al formular los estándares legales y personas inocentes pagarán el precio tarde o temprano.

D. Conclusión preliminar

16. Según el Tribunal, se requiere desde el principio la participación de una autoridad independiente[79], es decir, una que es independiente del ejecutivo, para evaluar el fin de la interceptación, la selección de los portadores[80] y las categorías de selectores[81], en el contexto de los principios de necesidad y proporcionalidad. La elección de selectores fuertes vinculados a individuos identificables es particularmente problemática, ya que la selección y el "uso de cada selector fuerte"[82] no requiere una autorización previa

[64] Párrafo 348 de la presente Sentencia.
[65] Párrafo 330 de la presente Sentencia.
[66] Párrafo 350 de la presente Sentencia.
[67] Ibíd.
[68] Ibíd.
[69] Párrafo 351 de la presente Sentencia.
[70] Párrafo 352 de la presente Sentencia
[71] Párrafo 355 de la presente Sentencia
[72] Ibíd.
[73] Párrafo 356 de la presente Sentencia.
[74] Párrafo 359 de la presente Sentencia.
[75] Párrafo 350 de la presente Sentencia.
[76] Párrafo 348 de la presente Sentencia.
[77] Párrafo 360 de la presente Sentencia.
[78] Ver, por ejemplo, el párrafo 370 *in fine* de la presente Sentencia
[79] Si bien el lenguaje del Tribunal no es uniforme, en ocasiones se hace referencia al concepto de autoridad independiente y otras veces a la de organismo independiente, parece que no hay diferencia sustancial entre estos conceptos.
[80] Párrafo 352 de la presente Sentencia.
[81] Párrafo 354 de la presente Sentencia.
[82] Párrafo 355 de la presente Sentencia.

independiente. Para el Tribunal, la autorización interna es suficiente en este caso, aunada a la garantía de que la solicitud de un selector fuerte está justificada y el proceso interno es registrado "escrupulosamente"[83].

17. Además, la ejecución de la orden de interceptación, incluyendo sus renovaciones posteriores, el uso, almacenamiento, transmisión posterior y eliminación de los datos obtenidos, deben ser supervisados por una autoridad independiente del ejecutivo, manteniéndose registros detallados en cada etapa del proceso para facilitar su supervisión[84].

18. Al final, la revisión *ex post facto* de todo el proceso debe ser realizada por una autoridad independiente del ejecutivo, de manera justa y mediante un procedimiento contradictorio, con facultades vinculantes para ordenar el cese de la interceptación ilícita y la destrucción del material obtenido o datos almacenados ilícitamente, así como de los datos obsoletos, equívocos o desproporcionados[85].

CONSTRUCCIÓN DE UN RÉGIMEN DE INTERCEPTACIÓN MASIVA *PRO PERSONA*

A. Interceptación masiva de comunicaciones

19. Considero que el régimen antes mencionado no equivale a un conjunto suficiente de garantías de los derechos de los artículos 8 y 10. En mi opinión, ha llegado el momento de no prescindir de las garantías fundamentales de autorización judicial, supervisión y control *ex post facto* en el ámbito de la interceptación masiva[86]. Como cuestión principal, el sistema judicial de supervisión de extremo a extremo de la interceptación masiva está justificado por la naturaleza extremadamente intrusiva de este proceso. No veo por qué un Estado regido por el estado de derecho no confía en sus jueces en servicio, en última instancia, en sus más antiguos y experimentados jueces, para decidir sobre tales asuntos. A menos que el Tribunal crea que los órganos asimilados a los judiciales son más independientes que los tribunales ordinarios... Desde este punto de vista, la independencia de los órganos asimilados a los judiciales no es un hecho. Además, si los tribunales ordinarios son competentes para autorizar, fiscalizar y revisar la interceptación de comunicaciones en procesos penales de alta complejidad, como las investigaciones sobre crimen organizado y terrorismo, no comprendo por qué no deberían ser competentes para realizar exactamente la misma función respecto a un proceso de interceptación masiva. Por lo tanto, ni la independencia ni la competencia de los tribunales ordinarios deben ser cuestionadas a los efectos de la construcción de un sistema de salvaguardas para el cumplimiento del Convenio en relación con el régimen de interceptación masiva. Un Estado que cree que el poder judicial en servicio no es apto para desempeñar estas funciones tiene un grave problema con el estado de derecho.

[83] Ibíd. Como el informe de la Comisión de Venecia, citada anteriormente, p. 28, dice, "los controles internos son insuficientes". Así, el párrafo 199 de la sentencia tergiversa la posición de la Comisión de Venecia.
[84] Párrafo 356 de la presente Sentencia.
[85] Párrafo 359 de la presente Sentencia.
[86] Informe de la Comisión de Venecia, citado anteriormente, pág. 32 ("Para los estados europeos, se prefiere la aprobación judicial *ex ante* en casos individuales"). Así, el párrafo 197 de la sentencia distorsiona el mensaje de la Comisión de Venecia. El Comisionado del Consejo de Europa Derechos Humanos también sugirió adoptar la autorización judicial *ex ante* (Memorándum, citado supra, § 28).

20. Sin duda, la intervención judicial no es la panacea[87]. Es obvio que la supervisión judicial de todo el proceso no tendría sentido si las categorías de delitos y actividades a sujetos a monitorización en la interceptación no se establecieran en la legislación interna con el grado de claridad y precisión necesario. En consecuencia, el control judicial debería abarcar la elección de los portadores específicos y selectores fuertes. Por específico me refiero a portadores individuales y selectores fuertes, no a "clases" o "categorías" de portadores o selectores, lo que supondría un cheque en blanco a la autoridad interceptora para recoger lo que quisiera.

21. En el caso de un sistema de doble bloqueo, por el cual el juez considere órdenes decididas previamente por un político o un funcionario administrativo, la supervisión judicial no debe limitarse a la posibilidad de invalidar la decisión administrativa cuando el juez considere que el político o el funcionario actuó irrazonablemente. Esto no sería verdaderamente una autorización judicial desde el test de necesidad y proporcionalidad exigido por el Convenio que es más exigentes que el test de mera razonabilidad.

22. Como mencioné en el asunto *Szábo y Vissy*, el Convenio no permite las expediciones de "pesca de datos" o "exploratorias", ni en forma de vigilancia no dirigida basada en selectores no específicos, ni en forma de vigilancia basada en selectores fuertes dirigidos a las comunicaciones del sujeto objetivo de la intercepción[88]. Tampoco es admisible ampliar la red de interceptación de sujetos mediante el despliegue de términos de búsqueda más difusos. Me gustaría recordar la razón fundamental por la que he llegado a esta conclusión. Admitir la interceptación masiva no dirigida implica un cambio fundamental en cómo vemos la prevención e investigación de delitos y la recopilación de inteligencia en Europa, desde apuntar a un sospechoso que puede ser identificado hasta tratar a todos como sospechosos potenciales, cuyos datos deben ser almacenados, analizados y perfilados[89]. Por supuesto, el impacto de tal cambio en los inocentes podría eventualmente ser mitigado por una cohorte de árbitros más o menos flexibles y reguladores y una plétora de leyes y códigos de conducta más o menos convenientes, pero una sociedad construida sobre tales cimientos es más parecida a un Estado policía que a una sociedad democrática. Esto sería lo contrario de lo que padres fundadores querían para Europa cuando firmaron el Convenio en 1950.

23. Por lo tanto, cualquier objetivo de vigilancia siempre debe ser identificado o identificable de antemano sobre la base de una sospecha razonable. Para no dejar dudas, la intercepción masiva debe ser admisible solo sobre la base de selectores fuertes dirigidos a las comunicaciones desde y hacia el sujeto objetivo de la intercepción cuando exista una sospecha razonable de que él o ella está involucrado en categorías

[87] El hecho de que la autorización judicial no sea en sí misma una garantía suficiente contra el abuso no apoya la conclusión de que no sea necesaria. Se debe apuntar que la IPA introdujo la autorización judicial *ex ante*, pero este no es el lugar para discutir *ex professo* el estándar de revisión judicial introducido por la IPA, porque la Ley de 2016 no es aplicable ante el Tribunal.

[88] Véanse todos los documentos internacionales citados en mi voto particular a *Szábo y Vissy*, antes citada.

[89] Por eso creo que la recopilación masiva de datos de personas inocentes aceptada por el Tribunal en la presente sentencia contraviene los principios establecidos en *S y Marper c. el Reino Unido*, núms. 30562/04 y 30566/04, § 135, 4 de diciembre de 2008; *Shimóvolos c. Rusia*, núm. 30194/09, §§ 68 y 69, de 21 de junio de 2011; *MK c. Francia*, núm. 19522/09, § 37, 18 de abril de 2013; y la más importante, *Mustafa Sezgin Tanrıkulu c. Turquía*, citada anteriormente, §§ 57-59.

legalmente definidas de infracciones graves o actividades que son perjudiciales para la seguridad nacional sin que necesariamente tengan que ser penales[90].

24. El aval judicial debe extenderse a la autorización para la vigilancia de comunicaciones o de datos relacionados con las comunicaciones, incluidos los datos confidenciales, con la única excepción de los casos urgentes, cuando el juez competente no esté disponible de inmediato, en los que la autorización puede ser otorgada por un fiscal, sujeta a la posterior aprobación del juez competente.

25. La legislación interna debe prever un régimen específico de protección para las comunicaciones profesionales privilegiadas de parlamentarios, médicos, abogados y periodistas[91]. La recopilación masiva e indiscriminada de comunicaciones sin sospechas frustraría la protección de la información protegida y confidencial, lo que solo puede ser garantizado mediante la autorización judicial para la interceptación de tales comunicaciones cuando se presenten pruebas que sirvan de apoyo a la sospecha de la comisión de delitos graves o conductas que atenten contra la seguridad nacional en relación con estos profesionales[92]. Además, cualquier comunicación de estas categorías de profesionales al estar cubiertas por su secreto profesional, si son interceptadas por error, deben ser destruidas inmediatamente. La ley interna también debería prever la prohibición absoluta de cualquier interceptación de comunicaciones amparadas por el secreto religioso.

26. La supervisión judicial no debe detenerse al inicio del procedimiento de interceptación. Si el funcionamiento real del sistema de interceptación se oculta a la supervisión del juez, la intervención inicial de un juez podría ser fácilmente socavada y privada de cualquier efecto real, haciéndola meramente virtual, una salvaguarda engañosa. Por el contrario, el juez debe acompañar durante todo el proceso, con un examen regular y atento de la necesidad y proporcionalidad de la orden de interceptación, en vista de los datos de interceptación adquiridos. A menos que reciba retroalimentación constante de la autoridad interceptora, el juez autorizador no sabrá cómo se está utilizando la autorización. En caso de incumplimiento de la orden de interceptación, el juez debe poder ordenar su cese inmediato y la destrucción de los datos obtenidos ilegalmente. Lo mismo debe aplicarse en caso de falta de necesidad de

[90] Este es el estándar universal establecido en la Compilación de las Naciones Unidas de buenas prácticas sobre marcos y medidas legales e institucionales que aseguren el respeto a los derechos de las agencias de inteligencia en la lucha contra el terrorismo, incluida su supervisión, de 17 de mayo de 2010 (A/HRC/14/46): "Práctica 21. La ley nacional describe los tipos de medidas de recolección disponibles para los servicios de inteligencia; los objetivos permisibles de inteligencia; las categorías de personas y actividades que pueden ser objeto de inteligencia; el umbral de sospecha requerido para justificar el uso de medidas de recolección; las limitaciones de los periodos durante los cuales se pueden utilizar las medidas de recolección; y los procedimientos para autorizar, supervisar y revisar el uso de medidas de recopilación de inteligencia".

[91] Aparte de *Sanoma Uitgevers B.V. contra los Países Bajos* [GC], núm. 38224/03, §§ 90-92, 14 de septiembre de 2010, véase Agencia de los Derechos Fundamentales de la Unión Europea (FRA), Vigilancia
por los servicios de inteligencia: garantías y recursos de los derechos fundamentales en la UE, volumen II:
Perspectivas de campo y actualizaciones legales, 2017, p. 12: "Los Estados miembros de la UE deben establecer procedimientos legales específicos para salvaguardar el privilegio profesional de grupos tales como miembros del parlamento, miembros del poder judicial, abogados y profesionales de los medios de comunicación. La implementación de estos procedimientos debe ser supervisada por un organismo independiente".

[92] Informe de la Comisión de Venecia, antes citada, pág. 26.

continuar con la operación, por ejemplo, porque los datos obtenidos no son de interés para los fines perseguidos por la interceptación solicitada. Solo un juez investido con el poder de tomar tales decisiones vinculantes puede proporcionar una garantía efectiva de la licitud del material que se conserva. En resumen, el juez debe estar facultado para realizar una revisión periódica del funcionamiento del sistema, incluidos todos los registros de interceptación y documentos clasificados[93], con el fin de evitar una injerencia desproporcionada en los derechos previstos en los artículos 8 y 10.

27. Finalmente, la revisión *ex post* del uso de una orden de interceptación también debe activarse mediante la notificación a la persona objetivo. Cuando nada obstaculiza la notificación a la persona cuyas comunicaciones han sido interceptadas, le permitiría participar en un procedimiento judicial justo y contradictorio sobre el fundamento de dicha interceptación[94]. Es, por lo tanto, altamente especulativo, por decir lo mínimo, pretender que un sistema que no depende de la notificación al sujeto de la intercepción "puede ofrecer incluso mejores garantías de un procedimiento adecuado que un sistema basado en la notificación"[95]. A nadie le importan más los intereses del sujeto de la intercepción que al propio sujeto.

28. Cuando, por alguna razón, como los intereses de la seguridad nacional, no es posible notificar a la persona cuyas comunicaciones han sido interceptadas, no hay forma realista de que la persona conozca la medida de vigilancia adoptada en relación con él o ella. 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), la forma en que se ejecutó la orden de interceptación con el fin de determinar si los datos en cuestión fueron legalmente recolectados y si deben ser conservados o destruidos; el sujeto de la intercepción debe entonces estar representado por un abogado experto en privacidad.

29. Por último, pero no menos importante, los recursos para la supervisión humana y financiera y las capacidades deben coincidir con la escala de las operaciones que se supervisan, de lo contrario, todo el sistema será una mera fachada que cubrirá el discrecional proceso administrativo de las autoridades interceptoras.

B. Intercambio de datos interceptados con servicios de inteligencia extranjeros.

30. El Tribunal ha establecido un estándar de protección más bajo para el traslado a los servicios de inteligencia extranjeros de datos obtenidos mediante la interceptación

[93] Este es el estándar universal y europeo según lo establecido respectivamente por la Compilación de las Naciones Unidas, citada anteriormente ("Práctica 25. Existe una institución independiente para supervisar el uso de datos personales por parte de los servicios de inteligencia. Esta institución tiene acceso a todos archivos en poder de los servicios de inteligencia y tiene la facultad de ordenar la divulgación de información a las personas interesadas, así como la destrucción de archivos o información contenida en el mismo") y FRA, Vigilancia por servicios de inteligencia, citada arriba, p. 11 ("Los Estados miembros también deben otorgar a los órganos de supervisión la facultad de iniciar sus propias investigaciones, así como el acceso permanente, completo y directo a la información y los documentos para el cumplimiento de su mandato").

[94] *Szábo y Vissy*, antes citada, § 86. En la lógica de *Szábo y Vissy*, este es un requisito mínimo por encima de los criterios de *Weber y Saravia*. Sobre las ventajas del proceso de notificación "para frenar el uso excesivo", véase el informe de la Comisión de Venecia, citada arriba, p. 35, y los informes del Comisionado de Derechos Humanos del Consejo de Europa sobre Alemania 2015, pág. 17, y sobre Reino Unido, 2016, antes citada, p. 5.

[95] Párrafo 358 de la presente Sentencia.

masiva. En primer lugar, el Estado que transfiere no tiene la obligación de comprobar si el Estado receptor tiene un grado de protección comparable al suyo. Además, no es necesario solicitar, antes de cada transferencia, una garantía de que el Estado receptor, al recibir los datos, pondrá en marcha salvaguardas capaces de prevenir abusos e interferencias desproporcionadas[96]. Por tanto, el Tribunal no ha excluido la posibilidad de una transferencia masiva de datos a un servicio de inteligencia exterior mediante un proceso continuo basado en un único fin. En vista de este marco altamente discrecional, no está claro en que consiste el "control independiente" requerido por el Tribunal[97]. ¿Cuál es el fin del control independiente si no hay necesidad de evaluar las salvaguardas establecidas por el Estado receptor (incluso en el sentido de "garantizar el almacenamiento seguro del material y restringir su ulterior divulgación"[98]) antes de cada transferencia? ¿Está limitado el control independiente a los casos en los que "está claro que el material requiere una confidencialidad especial - como el material periodístico confidencial -"[99]? ¿A quién debería quedar claro esto al servicio de inteligencia que lo transfiere o al juez? ¿Existe alguna diferencia entre control independiente y autorización independiente? La vaguedad del lenguaje del Tribunal parece servir a la dilución intencionada de las salvaguardas específicas relativas a la transferencia.

31. No veo ninguna razón para esta reducción de la protección del Convenio en caso de del intercambio de datos masivos, y el Tribunal tampoco proporciona ninguna. Según las normas consolidadas del Consejo de Europa y la Unión Europea, el intercambio de datos personales debe limitarse a terceros países que ofrezcan un nivel de protección esencialmente equivalente al garantizado dentro del Consejo de Europa y la Unión Europea, respectivamente[100]. En este caso, la supervisión judicial debe ser tan exhaustiva como en cualquier otro caso. Esta atenta supervisión judicial está particularmente justificada cuando un Estado miembro del Consejo de Europa está transfiriendo datos a un Estado no miembro, razón obvia por la que el uso futuro de esos datos por parte del Estado no miembro no está bajo la jurisdicción del Tribunal. Dicha supervisión judicial debería estar limitada por la "regla de terceros", según la cual está prohibido para una autoridad de inteligencia que recibió datos de un servicio de inteligencia extranjero compartirlos con un tercero sin el consentimiento de quien los originó[101].

---

[96] Párrafo 362 de la presente Sentencia.
[97] Ibíd.
[98] Ibíd.
[99] Ibíd.
[100] La mayoría ignora el hecho de que el artículo 2 del Protocolo Adicional del Convenio para la Protección de las Personas con respecto al Tratamiento Automático de Datos Personales, con respecto a las autoridades de supervisión y los flujos de datos transfronterizos (ETS n.º 181), establece que las partes deben garantizar un nivel adecuado de protección para las transferencias de datos personales a terceros países, y que las derogaciones sólo se admiten cuando existen intereses legítimos. El Informe Explicativo de dicho Convenio agrega que las excepciones deben ser interpretadas de manera restrictiva, "para que la excepción no se convierta en la regla general" (§ 31). Es importante señalar que este Protocolo ha sido ratificado por 44 Estados, incluidos 8 no miembros del Consejo de Europa. Reino Unido no lo ha ratificado. Además de este estándar del Consejo de Europa, la Unión Europea solo permite la transferencia de datos personales a un tercer país que ofrezca un nivel de protección esencialmente equivalente al garantizado dentro de la Unión Europea (§ 234 de esta sentencia).
[101] Informe de la Comisión de Venecia, citado anteriormente, 2015, p. 34 ("El autor o "tercera regla" no debe aplicarse al organismo de supervisión"), así como FRA, Vigilancia por inteligencia servicios, citado anteriormente, 2017, págs. 13 y 106 ("Sin perjuicio de la regla del tercero, los Estados miembros de la UE

C. Interceptación masiva de datos relacionados con las comunicaciones.

32. Finalmente, el Tribunal ha reconocido el potencial altamente intrusivo de la interceptación masiva de datos relacionados con las comunicaciones[102], pero ha fallado proporcionándoles el mismo grado de protección[103]. Por un lado, requiere que "las salvaguardas antes mencionadas [estén] establecidas", refiriéndose a las previstas en el apartado 361 de la Sentencia, pero por otro lado admite que los Estados miembros tienen la facultad discrecional de elegir qué salvaguardas específicas deben estar consagradas en la legislación nacional, ya que "las disposiciones que rigen ... el tratamiento [de los datos relacionados con las comunicaciones] no necesariamente tienen que ser idénticas en todos los aspectos a las que gobiernan el tratamiento del contenido"[104] . El mensaje borroso del Tribunal es tan ambiguo que no proporciona una orientación adecuada a los Estados en cuanto a cuáles de las "salvaguardas mencionadas" son obligatorias, si es que las hay, para la interceptación masiva de datos relacionados con las comunicaciones. En consecuencia, la postura vacilante del Tribunal no alivia el riesgo de mapear la vida social completa de una persona que el propio Tribunal ha identificado.

D. Conclusión preliminar

33. No estoy de acuerdo con que "los Estados disfruten de un amplio margen de apreciación para decidir qué tipo de régimen de interceptación es necesario para estos fines [para proteger la seguridad nacional y otros intereses nacionales esenciales contra amenazas externas graves], [pero] en el funcionamiento de un sistema de este tipo el margen de apreciación que se les concede debe ser más limitado"[105]. Si los límites a las facultades discrecionales del Estado son amplios, incluso la vigilancia policial más estricta es insuficiente para protegerse contra el abuso. El margen de apreciación debe ser el mismo, tanto para el diseño del sistema como para su funcionamiento, y este margen es estrecho, en vista de la naturaleza profundamente intrusiva de los poderes de vigilancia estatales en cuestión, el riesgo inherentemente alto de abuso de estos poderes y - que no se nos olvide- el consenso europeo sobre la prohibición de interceptación masiva no dirigida. Este riesgo se ve magnificado por algunos gobiernos obsesionados con la seguridad con un apetito ilimitado por los datos que ahora tienen los medios tecnológicos para controlar la comunicación digital mundial.

34. En suma, el derecho interno debe ser suficientemente claro en sus términos para dar a las personas físicas y jurídicas[106] una indicación adecuada de las condiciones obligatorias y procedimientos multinivel según los cuales las autoridades están

---

deberían considerar la posibilidad de otorgar a los organismos de supervisión acceso completo a los datos transferidos a través de la cooperación internacional. Esto ampliaría los poderes de supervisión sobre todos los datos disponibles y procesados por los servicios de inteligencia").

[102] Párrafo 342 de la presente Sentencia.

[103] En definitiva, el Tribunal fue sensible a la amenaza del Gobierno, según la cual "si se requiriera que los estados miembros que operaban un régimen de interceptación masiva aplicaran el mismo protecciones a RCD [datos relacionados con las comunicaciones], que, al contenido, entonces el resultado probable sería simplemente una dilución de la protección del contenido". (Alegaciones del Gobierno demandado ante la Gran Sala de 2 de mayo de 2019, p. 42).

[104] Párrafo 364 de esta Sentencia en relación con el párrafo 361.

[105] Párrafo 347 de la presente Sentencia.

[106] En *Liberty y otros*, citada anteriormente, todos los demandantes eran ONGs que argumentaban que el derecho a la protección de su correspondencia había sido violado. Estos derechos también están comprometidos en el presente caso.

autorizadas a recurrir a la interceptación masiva; estas condiciones y procedimientos incluyen los siguientes[107]:

(a) La definición de los motivos que pueden justificar la adopción de una orden de interceptación, tales como: la detección de actividades que supongan una amenaza para la seguridad nacional o la prevención, detección o investigación de delitos graves, en cuyo caso las infracciones que puedan desencadenar la interceptación deberán corresponder a una lista de infracciones graves específicas o, en general, a delitos punibles con cuatro o más años de prisión[108].

(b) Una definición de los sujetos a interceptar, en otras palabras, las personas o instituciones que puedan ver sus comunicaciones interceptadas, como sigue:

> (i) prohibición estricta de la pesca de datos o expediciones exploratorias, para descubrir "incógnitas desconocidas", incluida cualquier forma de vigilancia no dirigida basada en selectores no específicos,
>
> (ii) prohibición estricta del uso de selectores fuertes destinados a comunicaciones sobre el sujeto objeto de la intercepción,
>
> (iii) admisibilidad de selectores firmes dirigidos a las comunicaciones desde y hacia el sujeto objeto de la interceptación cuando hay una sospecha razonable de que el sujeto interceptado está involucrado en los delitos o actividades mencionados anteriormente.

(c) Un catálogo de las formas de comunicaciones electrónicas que pueden ser interceptadas, como teléfono, télex, fax, correo electrónico, búsquedas de Google, navegaciones por Internet, las redes sociales y el almacenamiento en la nube.

(d) La observancia del principio de necesidad, que exige que:

> (i) la interferencia con los derechos de los sujetos interceptados debe servir adecuadamente a los objetivos perseguidos y no ir más allá de lo necesario para alcanzarlos;
>
> (ii) la interceptación debe justificarse únicamente como una medida de último recurso, es decir, cuando no se dispone de otros medios para obtener pruebas o información, cuando el recurso a otros métodos menos intrusivos ha resultado infructuoso o, excepcionalmente, si se considera poco probable que otros métodos menos intrusivos tengan éxito;
>
> (iii) la interceptación debe adaptarse para evitar, en la medida de lo posible, apuntar a personas o instituciones que no sean responsables de los delitos o actividades antes mencionados; y
>
> (iv) la intercepción debe detenerse inmediatamente cuando ya no sirva a los fines perseguidos.

(e) La observancia del principio de proporcionalidad, que requiere que:

---

[107] Con este fin, además de los documentos mencionados en el párrafo 8, también he teniendo en cuenta la Compilación de las Naciones Unidas, antes citada, 2010, el Informe de la Comisión de Venecia, citado anteriormente, 2015, y el informe de la FRA, citado anteriormente, 2017.

[108] El artículo 2 (b) del Convenio de las Naciones Unidas contra la Delincuencia Organizada Transnacional define "Delito grave" como conducta punible con una privación máxima de libertad de al menos cuatro años o una pena más grave. El Informe explicativo de la Recomendación Rec (2005) 10 del Comité de Ministros sigue esa referencia.

(i) debe lograrse un justo equilibrio entre los derechos contrapuestos de los sujetos interceptados y los fines perseguidos, de acuerdo con el principio de que cuanto más grave sean las infracciones o actividades antes mencionadas y sus consecuencias pasadas o futuras, más intrusiva y extensa puede ser la interceptación; y

(ii) en todo caso la interceptación debe asegurar la esencia (o núcleo mínimo) de los derechos de los sujetos interceptados, como el derecho a la intimidad de la vida privada en el caso de las personas físicas. La interceptación debe cesar tan pronto como se hace evidente que está invadiendo el núcleo de la vida privada.

(f) Un límite a la duración de la orden de interceptación, que puede ser prorrogado una o más veces después de una evaluación de los resultados de la operación, pero en todo caso con un plazo máximo impuesto para la toda la operación.

(g) Supervisión judicial de extremo a extremo, lo que incluye:

(i) autorización de interceptación, incluyendo los portadores específicos a ser interceptados y selectores fuertes a utilizar;

(ii) el control periódico de la ejecución de la orden de interceptación, en intervalos suficientemente cortos, incluida la extensión de la duración de la orden de intercepción y de la transmisión de los datos obtenidos a terceros; y

(iii) revisión *ex post facto* del proceso de interceptación y de los datos interceptados.

(h) En casos de urgencia, la orden de interceptación especial puede ser concedida por un fiscal, pero debe ser confirmada por un juez dentro de un breve período de tiempo.

(i) El procedimiento a seguir para examinar, usar, almacenar y destruir los datos obtenidos, con una descripción detallada del alcance de la supervisión del juez durante la etapa de ejecución y cuando la interceptación haya terminado y la documentación de los pasos clave de la supresión de los datos en todo lo que sea necesario para la supervisión del juez.

j) Las condiciones que deben cumplirse y las precauciones que deben tomarse al intercambiar datos interceptados con servicios de inteligencia extranjeros, éstas son:

(i) una prohibición absoluta de subcontratar operaciones de vigilancia para eludir las reglas nacionales;

(ii) una prohibición absoluta para una autoridad de inteligencia que recibió datos de un servicio de inteligencia extranjero de compartirlos con un tercero sin el consentimiento de quien los interceptó, esta regla no limita el acceso del juez interno del Estado receptor a los datos transferidos;

(iii) una prohibición absoluta de intercambiar datos con servicios de inteligencia extranjeros que no garantizan un nivel de protección esencialmente equivalente al garantizado por el Convenio;

(iv) una prohibición absoluta de transferencia masiva de datos a o de recibirlos de un servicio extranjero de inteligencia mediante un proceso continuo basado en un solo fin;

(v) una autorización judicial previa a cada transferencia / recepción de datos de conformidad con exactamente los mismos principios y reglas de la interceptación masiva nacional, que incluyen, entre otros, la observancia de los principios de necesidad y proporcionalidad;

(vi) estas reglas se aplican sin distinción entre datos solicitados y no solicitados, datos en “bruto” (no evaluados) y datos evaluados.

(k) El deber de notificar al sujeto la interceptación cuando ésta ha terminado, salvo cuando los intereses de la seguridad nacional estén en peligro por dicha divulgación, en cuyo caso el juez competente deberá estar facultado para revisar por iniciativa propia (*ex proprio motu*) o por iniciativa de un tercero (por ejemplo, un fiscal) todo el proceso de interceptación para determinar si los datos fueron obtenidos legalmente y si deben ser conservados o destruidos, el sujeto interceptado deberá ser defendido por un abogado experto en privacidad.

(l) Garantías especiales en cuanto al secreto de las comunicaciones de sujetos privilegiados como parlamentarios, médicos, abogados, periodistas y sacerdotes.

(m) La garantía de que una condena penal no puede basarse únicamente o en una medida decisiva en una evidencia recopilada por medio de la interceptación masiva.

(n) Estos principios se aplican a la vigilancia realizada en el territorio propio de la Parte Contratante, así como a la vigilancia realizada extraterritorialmente, independientemente del fin de la vigilancia, el estado de los datos (almacenados o en tránsito), o la posesión de los datos (datos retenidos en posesión del sujeto interceptado o en posesión de un proveedor de servicios).

o) La obligación del Estado de respetar y garantizar los derechos de las personas se ve complementada con la obligación de proteger los derechos de las personas frente a los abusos de agentes no estatales, incluidas las entidades empresariales.

IV. CRÍTICA AL RÉGIMEN DE INTERCEPCIÓN MASIVA DEL REINO UNIDO IMPUGNADO

A. Interceptación masiva de comunicaciones en el marco de la RIPA 2000

35. Teniendo en cuenta lo anterior, tengo una objeción de principios, mucho más allá del tenue desafío de la Gran Sala al grueso del régimen de interceptación del Reino Unido, tal como estaba el 7 de noviembre de 2017, lo que significa antes de la plena entrada en vigor de la Ley de Poderes de Investigación de 2016 (IPA)[109].

36. El fin de la interceptación masiva de detectar e investigar delitos graves como se define en la sección 81 (2) b de la RIPA definitivamente no es compatible con el concepto de delito grave imperante en el derecho internacional, en la medida en que el concepto interno engloba los delitos punibles con prisión por un período inferior a cuatro años. Además, el fin de salvaguardar el bienestar económico del Reino Unido en la medida en que esos intereses también sean relevantes para los intereses de la seguridad nacional no es suficientemente preciso, lo que permite utilizar la interceptación masiva, por ejemplo, para fines económicos y espionaje industrial y con fines de "guerra comercial"[110]

[109] Párrafo 270 de la presente Sentencia. Esto significa que, al igual que la Gran Sala, no he tenido en cuenta los cambios introducidos por la IPA y el nuevo Código IC de 2018. No eran aplicables ante este Tribunal.

[110] Véase el interesante debate entre las partes durante la vista ante la Gran Sala del 10 de julio de 2019 sobre este punto exacto. El Tribunal ha defendido diferentes puntos de vista sobre la precisión del fin de seguridad nacional (comparar y contrastar *Iordachi y Otros c. Moldova*, núm. 25198/02, § 46, 10 de febrero de 2009, y *Kennedy c, Reino Unido*, citada anteriormente, § 159).

37. Los términos muy generales de la sección 8 (4) respecto a los certificados del Secretario de Estado también fueron reprochados, y con razón, por el Comité de Inteligencia y de Seguridad del Parlamento (ISC)[111].

38. La distinción entre comunicaciones internas y externas, tal como se establece en la sección 20 de la RIPA, es fundamentalmente defectuosa y no circunscribe las categorías de personas cuyas comunicaciones son susceptibles de ser interceptadas. Como concluyó el ISC, esta distinción era confusa y carecía de transparencia[112].

39. La justificación del Gobierno para esta distinción era que "[c]uando se adquiere inteligencia sobre actividades en el extranjero, los Servicios de Inteligencia no tienen la misma capacidad para identificar objetivos o amenazas que poseen dentro el Reino Unido"[113]. El IPT reiteró el argumento, afirmando que "era más difícil investigar amenazas terroristas y criminales del exterior"[114]. Esta justificación debe entenderse en el contexto de las divulgaciones del Gobierno de 2014, que reconocieron que las solicitudes masivas de material fueron hechas a un servicio de inteligencia extranjero "de otra manera que de conformidad con un acuerdo internacional de asistencia judicial recíproca"[115]. Así, el sistema de interceptación masiva impugnado fue creado para evitar los largos y costosos procedimientos y obligaciones "más duras" derivadas del marco de derecho internacional existente en materia de asistencia judicial recíproca, en otras palabras, para eludir las salvaguardas bajo el sistema de acuerdos de asistencia mutua existentes y aprovechar la falta de regulación de las nuevas tecnologías de vigilancia transnacional.

40. Además, con una cantidad cada vez mayor de comunicaciones que son tratadas como externas[116], y el aumento exponencial de la interceptación masiva de cada vez más comunicaciones de personas que están en el Reino Unido[117], la distinción entre comunicaciones externas e internas simplemente no es técnicamente factible de sostener y, por lo tanto, no tiene sentido. La distinción de la jurisdicción territorial basada en comunicaciones externas e internas es inherentemente contradictoria con la realidad del flujo actual de comunicaciones en Internet, donde se intercambia un mensaje de Facebook dentro de un grupo de amigos en Londres que se enruta a través de California y, por lo tanto, es "externo" al Reino Unido[118]. Como recordó la Sociedad de Abogados al Tribunal, las comunicaciones confidenciales entre abogados y clientes, incluso cuando ambos estaban en el Reino Unido, podían ser interceptadas bajo el régimen de la sección 8 (4)[119]. En la práctica, el concepto expansivo de comunicaciones externas del Gobierno también incluye el almacenamiento en la nube, búsquedas de Google,

[111] Párrafo 146 de la presente Sentencia.
[112] Párrafo 145 de la presente Sentencia.
[113] Véanse las alegaciones del Gobierno demandado ante la Gran Sala de 2 de mayo 2019, pág. 9
[114] Párrafo 51 de la presente Sentencia, que el Tribunal reiteró en el párrafo 375.
[115] Párrafos 36 y 116 de la presente Sentencia, que remiten al párrafo 12.2 del Código IC.
[116] Párrafo 47 de la presente Sentencia.
[117] Como dijo el Gobierno demandado: "Pero el hecho de que las comunicaciones electrónicas tomen cualquier ruta para llegar a su destino significa inevitablemente que una proporción de las comunicaciones que fluyan sobre un portador entre el Reino Unido y otro Estado consistirán en 'comunicaciones internas': es decir, comunicaciones entre personas ubicadas en el Reino Unido." (ver sus alegaciones ante la Gran Sala de 2 de mayo de 2019, p. 20
[118] Párrafo 75 de la presente Sentencia.
[119] Párrafo 321 de la presente Sentencia. Véase también la sentencia del IPT *Belhadj y otros c. Servicio de seguridad y otros*, IPT / 13 / 132-9 / H. 120

actividades de navegación y redes sociales[120]. Para muchos tipos de comunicaciones, puede que ni siquiera sea posible distinguir entre comunicaciones externas e internas, ya que la ubicación prevista del destinatario no siempre es evidente a partir de los datos relacionados con las comunicaciones. El análisis fáctico de si una comunicación en particular es externa o interna solo se puede llevar a cabo con el beneficio de la retrospectiva[121]. La interconexión más estrecha de las condiciones de vida de hoy en día a las comunicaciones a través de las fronteras ciertamente no es un argumento para el tratamiento de comunicaciones externas e internas de manera diferente, sino al contrario. Esto, por supuesto, no debe entenderse como una invitación a bajar el nivel de protección de las comunicaciones internas, sino a aumentar el nivel de protección de las comunicaciones externas.

41. Al respecto, no es evidente que una comunicación entre una persona en Estrasburgo y una persona en Londres deba tener derecho a una protección más limitada en virtud del Convenio que una comunicación entre dos personas en Londres. Por tanto, no parece haber ninguna justificación objetiva para tratar a tales personas de manera diferente, aparte de la suposición de que las amenazas provienen la mayoría de las veces del exterior, y que los extranjeros son menos dignos de confianza que los nacionales, porque representan un riesgo más grave a la seguridad nacional y la seguridad pública que los nacionales, lo que justifica la necesidad de monitorear las comunicaciones enviadas o recibidas fuera de las Islas Británicas[122]. Esto también se refleja en la forma en que se trata a los extranjeros en los tribunales cuando quieren defender su derecho a la privacidad. El IPT no acepta reclamaciones de demandantes fuera del territorio nacional[123]. Esta *Weltanschauung* hostil a los extranjeros no podría ser más ajena al espíritu y letra del Convenio[124]. El Convenio pone en el centro al individuo, no al ciudadano de un Estado, lo que significa que los derechos del Convenio como derechos del individuo deben brindar protección cada vez que una Parte Contratante actúa y, por lo tanto, crea potencialmente una necesidad de protección, independientemente de dónde, hacia quién y de qué manera lo hace. Además, los derechos del Convenio deben

[120] Párrafo 75 de la presente Sentencia. Esta práctica parece contradecir el párrafo 6.5 del Código IC.

[121] El propio Gobierno demandado lo admitió (véanse sus alegaciones ante el Gran Sala de 2 de mayo de 2019, p. 37).

[122] No basta con argumentar que, dado que la legislación británica "impide que el material interceptado sea seleccionado para su examen de acuerdo con un factor "referible a un individuo que se sabe que se encuentra por el momento en las Islas Británicas, cualquier diferencia de trato no se basaría directamente en la nacionalidad o el origen nacional, sino más bien en la ubicación geográfica", como hizo la sentencia de la Sala (§ 517), por la razón obvia por la que la gran mayoría de las personas que se sabe que están por el momento en las Islas Británicas son ciudadanos británicos y viceversa, la mayoría de los que están fuera son extranjeros. Cuanto más el tratamiento beneficioso de los nacionales también fue señalado por la FRA (Vigilancia por inteligencia servicios, citado anteriormente, pág. 45: "Cuando los servicios de inteligencia realizan vigilancia a nivel nacional, las garantías legales aplicables se mejoran en comparación con las vigentes para la vigilancia extranjera")

[123] IPT, *Human Rights Watch & Ors c. SoS for the Foreign & Commonwealth Office & Ors*, 16 de mayo de 2016: "Con respecto a cualquier creencia afirmada de que cualquier conducta incluida en la sección 68 (5) de la RIPA se ha llevado a cabo por o en nombre de cualquiera de los Servicios de Inteligencia, el demandante debe demostrar que existe una base para tal creencia, de modo que pueda demostrar que está potencialmente en riesgo de ser sometido a tal conducta. Además, dicho demandante debe demostrar que está o estuvo en ese momento material presente en el Reino Unido".

[124] Informe de la Comisión de Venecia, antes citado, pág. 17, hace la misma crítica "sobre motivos fundamentales", al igual que el Relator Especial de la ONU sobre la promoción del derecho a libertad de opinión y expresión, en referencia al Pacto Internacional de Derechos Civiles y Políticos (véase el párrafo 313 de esta sentencia).

impregnar la participación de los Estados miembros del Consejo de Europa en la comunidad internacional, en la medida en que "el orden jurídico del Consejo de Europa ya no puede confundirse con el tradicional acuerdo internacional de egoísmos yuxtapuestos. La soberanía ya no es un hecho absoluto, como en los tiempos de Westfalia, sino una parte integral de una comunidad defensora de los derechos humanos"[125].

42. Al final, la distinción de la RIPA no era apta para su fin en la era del desarrollo de Internet y solo sirvió al objetivo político de legitimar el sistema a los ojos del pueblo británico con la ilusión de que las personas dentro de la jurisdicción territorial del Reino Unido se ahorrarían el "Gran Hermano" gubernamental. De hecho, no era así. El Secretario de Estado podía, cuando lo considerara necesario, determinar el examen de material seleccionado de acuerdo con factores atribuibles a un individuo que se encontrara en las Islas Británicas[126] y modificar un certificado para autorizar la selección de comunicaciones de ese individuo[127]. Además, la captura incidental de comunicaciones no identificadas en la orden del Secretario de Estado estaba permitida siempre que fuera necesaria para obtener las comunicaciones externas que eran objeto de la orden[128], y según el propio Gobierno, esto "en la práctica era inevitable"[129]. Dicho esto, cabe señalar que, en relación con la interceptación masiva de datos relacionados con las comunicaciones, ni siquiera hubo restricción a las comunicaciones externas.

43. Incluso si la interceptación masiva estuviera destinada a ser un poder para reunir inteligencia extranjera[130], más que una herramienta para la prevención, detección e investigación del crimen[131], esto no justifica la falta de regulación o la amplitud de los poderes de las autoridades de interceptación. En cualquier caso, como resultado del desarrollo de las comunicaciones digitales, la salvaguarda de las comunicaciones externas ya no actúa como una restricción significativa[132], si es que alguna vez lo hizo. Mi punto de vista es que nunca lo hizo, por las siguientes razones.

44. El Secretario de Estado no proporcionaba ninguna autorización independiente para la orden de la sección 8 (4)[133], siendo su orden de interceptación un cheque en blanco, que ni nombraba ni describía al sujeto de la intercepción, no imponía un límite expreso en el número de comunicaciones que podían ser interceptadas, y no especificaba ni portadores ni selectores. Ninguna disposición específica se aplicaba al supuesto en el que hubiera una solicitud de comunicaciones de un periodista, o un médico, o un sacerdote, o cuando tal intrusión colateral era probable, más allá de los inocuos párrafos 4.28 al 4.31 del Código IC[134]. La elección de portadores y la aplicación de selectores,

[125] Párrafo 22 de mi voto particular en *Mursić c. Croacia* [GC], núm. 7334/13, 20 de octubre de 2016.
[126] Sección 16 (3) de la RIPA.
[127] Párrafo 6.2 del Código IC.
[128] Sección 5 (6) (a) de la RIPA y párrafo 6.6 del Código IC.
[129] Alegaciones del Gobierno demandado ante la Gran Sala de 2 de mayo de 2019, pág. 37.
[130] De acuerdo con el párrafo 6.2 del Código IC, "la interceptación de la sección 8 (4) es una facultad de recolección".
[131] La sección 81 de la RIPA define la prevención y detección de delitos, pero no la investigación.
[132] Informe de la Comisión de Venecia, antes citado, pág. 11, hace la misma apreciación.
[133] El Parlamento del Reino Unido reconoció, en su informe ISC de 2015, la falta de independencia de la Secretaría de Estado, antes del cambio de la IPA en 2016.
[134] Disposiciones aplicables al material de la sección 8 (4) que se selecciona para examen y que constituye información confidencial (párrafo 4.32 del Código IC). El Gobierno demandado ahora reconoce "que las solicitudes de datos de comunicaciones destinadas a identificar fuentes periodísticas deben estar sujetas a

incluidos selectores fuertes, a las comunicaciones externas dependía de la última palabra de la autoridad interceptora[135]. En palabras llanas, la comunidad de inteligencia tenía el control total del procedimiento de autorización, manteniendo al Secretario de Estado lejos de la información esencial, con la consecuencia de que podía no realizar un análisis adecuado de la proporcionalidad y la necesidad, sino blanqueado políticamente el funcionamiento del sistema[136].

45. Además, el Código de prácticas emitido por el Secretario de Estado no era vinculante, pues permitía apartarse de él por razones justificadas. Peor aún, el trabajo diario de los analistas se regía por las disposiciones por "debajo de la línea de flotación", que no estaban disponibles para el público, ni de forma somera ni de forma expresa[137]. Este margen de maniobra administrativo de la autoridad de interceptación derrotó el fin del principio de legalidad, según el cual las reglas que rigen la interceptación masiva deben tener una base en el derecho interno y dicha ley debe ser accesible y previsible en cuanto a sus efectos.

46. La debilidad normativa del sistema se vio agravada por el estatus del Comisionado de Interceptación de Comunicaciones (Comisionado IC), que no era una autoridad independiente ni realizaba una supervisión efectiva de la implementación de la orden de interceptación[138]. Como lo expresó el Informe ISC de 2015, "si bien los dos Comisionados son exjueces, en su papel de Comisionados operan fuera del marco judicial oficial", concluyendo que "actualmente varias de estas responsabilidades no se llevan a cabo de acuerdo con la normativa. Esto es insatisfactorio e inapropiado"[139]. Este no es el peor aspecto de la situación jurídica del Comisionado IC. Como cuestión de derecho, el Primer Ministro nombró al Comisionado IC, quien le reportaba y era dependiente del personal proporcionado por el Secretario de Estado[140]. Además, era un trabajo a tiempo parcial y el Comisionado IC podía ser despedido por el Primer Ministro en cualquier momento[141]. Este estatus evidentemente no era compatible con la independencia necesaria para una supervisión eficaz del funcionamiento del régimen de la sección 8 (4). En resumen, los Comisionados no eran "institucional, operativa y financieramente independientes de las instituciones que [tenían] el mandato de supervisar", como exigen los principios Tshwane[142].

---

aprobación judicial" (respuesta del Reino Unido al Comisionado de derechos humanos del Consejo de Europa - Memorando sobre vigilancia y supervisión mecanismos en el Reino Unido, pág. 24).

[135] Párrafos 146-147 de la presente Sentencia.

[136] Esta fue también la conclusión del informe ISC de 2015 (véase el párrafo 147 de esta sentencia). No es de extrañar entonces que en 2016, 3.007 órdenes de interceptación fueran emitidas y solo cinco solicitudes fueran rechazadas por el Secretario de Estado (párrafo 170 de esta sentencia). Las cifras lo dicen todo: el Secretario de Estado estaba allí solo para sellar las peticiones.

[137] Párrafo 33 de la presente Sentencia.

[138] Ver § 347 de la sentencia de la Sala, y § 26 del voto particular del Juez Koskelo, acompañado por el juez Turković, que señala el hecho de que el sistema del Reino Unido está de hecho detrás del sistema alemán de salvaguardas existente en la época de *Klass y otros y Weber y Saravia*.

[139] Lamentablemente, este pasaje del informe ISC de 2015, al que se hace referencia en el párrafo 142 de la sentencia, fue pasado por alto por la mayoría.

[140] Párrafo 57 de la RIPA 2000.

[141] La crítica realizada por la demandante durante la vista ante la Gran Sala el 10 de julio de 2019 es legítima: un solo juez jubilado que trabaja a tiempo parcial y con una pequeña secretaría y realizando un modesto análisis de muestras "no se puede esperar que ejerza una supervisión significativa".

[142] Sobre estos principios y su papel dentro del Consejo de Europa, ver mi voto particular en *Szábo y Vissy*, antes citada.

47. Incluso suponiendo, por el bien del debate, que la supervisión del Comisionado en el Reino Unido era independiente, no era eficaz, por la sencilla razón de que, cuando se enfrentaba a un grave error, el Comisionado solo tenía el poder de hacer un informe al Primer Ministro para señalar este error y, de ser así, para decidir en qué medida era posible publicar ese error[143]. Por ejemplo, no podía remitir el caso al IPT, ni notificarlo a la víctima de la interceptación excesiva. De hecho, ¡el Comisionado ni siquiera identificó que los demandantes Amnistía Internacional y el Centro de Recursos Legales de Sudáfrica habían sido sometidos a vigilancia ilegal!

48. La duración de los periodos de interceptación y plazos de retención no encontraban límite máximo de tiempo en la ley, y en la práctica no se colmaba esta laguna[144]. Las garantías de la sección 8 (4) podían renovarse *ad aeternum*[145]. Es más, los períodos de retención diferían entre las diferentes autoridades interceptoras[146] y el plazo máximo "normal" de conservación de conformidad con el párrafo 7.9 del Código IC (es decir, dos años) podía ser dispensado por un alto funcionario de la misma autoridad interceptora. Esto es una señal reveladora de quién dirigió el programa en el sistema británico de interceptación masiva[147].

49. No había obligación de notificación al final del proceso de interceptación[148]. A falta de tal notificación, el derecho de acceso a un tribunal era en gran parte inútil. Este era el caso del Reino Unido[149]. El IPT actuaba sólo ante una reclamación de una persona que creía que había sido sometida a vigilancia secreta, lo que significaba que el IPT era una garantía teórica para todos aquellos sujetos interceptados que no tenían idea alguna de que sus comunicaciones habían sido interceptadas[150]. La insuficiencia de la supervisión del IPT se vio agravada por el hecho de que no tenía poder para hacer una declaración de incompatibilidad si consideraba que la legislación primaria era incompatible con el CEDH, ya que no era un "tribunal" a los efectos de artículo 4 de la Ley de Derechos Humanos de 1998; que sus fallos no estaban sujetos a apelación; y, curiosamente, que el Secretario de Estado tenía el poder de adoptar las normas de procedimiento del IPT, lo que en la práctica significaba que la entidad supervisada tenía el poder de determinar las reglas que regían al órgano de control[151].

---

[143] Como reconoció el Gobierno demandado en la vista ante la Gran Sala 10 de julio de 2019.

[144] Según lo descrito por el Gobierno demandado (párrafo 403 de esta sentencia). Parece que incluso las políticas internas no se cumplen (párrafo 59 de esta Sentencia).

[145] Párrafos 6.22 a 6.24 del Código IC.

[146] Párrafo 176 de la Sentencia.

[147] Es bastante sorprendente que la mayoría, en el párrafo 405 de la sentencia, solo haya encontrado "deseable" que la práctica descrita por el Gobierno demandado ante la Gran Sala deba estar consagrada en la ley.

[148] La IPA introdujo un requisito para que el Comisionado considerara si ha habido un error grave y era de interés público notificar al individuo, pero esta regla no es aplicable ante el Tribunal en el presente caso. La elección de la política de la IPA es una concesión de que el sistema anterior era insuficiente, y será necesario más tiempo para ver si la solución IPA es suficiente.

[149] Esto se ve agravado por la política NCND ("ni confirmar ni negar") del Gobierno, que "impide que una persona sepa si ha sido objeto de vigilancia" y "protege las decisiones de vigilancia de un escrutinio efectivo", como concluyó Comisionado de Derechos Humanos del Consejo de Europa (Memorando, citado anteriormente).

[150] Por lo tanto, la conclusión de la mayoría de que el IPT es "un recurso judicial sólido para cualquiera que sospechaba que sus comunicaciones habían sido interceptadas" (§ 415) no identifica la patente deficiencia del sistema: su carácter virtual para aquellos que no tienen motivos para sospechar que han sido sometidos a vigilancia secreta.

[151] Sección 69 (1) de la RIPA.

B. Intercambio de datos interceptados por los servicios de inteligencia extranjeros.

50. No existe un marco legal expreso análogo a la RIPA que rija el poder en virtud del cual el gobierno británico puede utilizar datos interceptados por un país extranjero. Solo a partir de enero de 2016 el Capítulo 12 del Código IC establecería el marco de actuación para dicho intercambio[152]. Conforme al párrafo12.5 del Código IC, y la nota al pie que lo acompaña, las solicitudes de interceptación de comunicaciones y de los datos relacionados con las comunicaciones de un servicio de inteligencia extranjero podía llevarse a cabo para un "material hacía, desde y sobre selectores"[153]. La NSA abandonó la colección "sobre" en abril de 2017, porque no podía realizarse lícitamente dada su inadmisible extralimitación masiva[154]. Sin embargo, la sorprendente disposición del Tribunal al aceptar la política del gobierno demandado de "coleccionar todas"[155] va más allá incluso del libro de jugadas de la NSA, admitiendo no solo solicitudes de colección "sobre", sino incluso solicitudes para materiales distintos de los relacionados con selectores específicos[156].

51. Según el Tribunal, la transferencia masiva de material a socios de inteligencia extranjeros debe estar sujeta a un "control independiente"[157], pero la recepción masiva de material obtenido por autoridades de inteligencia extranjeras no[158]. Si las salvaguardas son inadecuadas en relación con la vigilancia directa por las autoridades de interceptación del Reino Unido, deberían ser consideradas inadecuadas también para la vigilancia indirecta por ellos, resultante del intercambio de material de inteligencia interceptado por terceros; más aún cuando dicho material era recopilado por un tercero que no estaba sujeto al Convenio. Pese a que en esos casos el peligro de que el material haya sido recolectado y almacenado de una manera que no cumple con el Convenio es más alto y, por lo tanto, su supervisión independiente es más necesaria, el Tribunal ha renunciado a esta salvaguarda, sin justificación alguna[159]. En este sentido, la supervisión del Comisionado IC y el IPT, invocados por el Gobierno y la mayoría de jueces de la Gran Sala, era prácticamente inoperante, en el control del intercambio de inteligencia con terceros de material interceptado no menos que en la supervisión de la vigilancia interna, ya que la intervención del IPT dependía de una reclamación y el Comisionado IC no tenía más facultades o atribuciones que la de realizar un informe para el Primer Ministro con la finalidad de poner en su conocimiento cualquier error grave.

---

[152] El Gobierno demandado dijo que, "incluso antes de la emisión del capítulo 12 del Código, era "accesible" como consecuencia de la divulgación", en referencia a la divulgación de octubre de 2014 (véanse sus alegaciones ante la Gran Sala de 2 de mayo de 2019, p. 49). Esto muestra que incluso el Gobierno admite que antes de ese momento la ley no era accesible.

[153] Párrafo 116 de la presente Sentencia.

[154] Párrafo 263 de la presente Sentencia.

[155] En palabras del Gobierno demandado en la vista ante la Gran Sala del 10 de julio 2019: "así que en la medida en que el aguijón de las preguntas es si se tienen muchos datos, incluso tras el proceso de filtrado, la respuesta a esa pregunta es "sí" y algo muy bueno también, nos sometemos".

[156] Párrafos 502 y 503 de la presente Sentencia.

[157] Párrafo 362 de la presente Sentencia.

[158] Párrafo 513 de la presente Sentencia.

[159] Lamentablemente, el Tribunal ignoró la posición del Comité de Derechos Humanos en sus Observaciones finales de 2015 sobre el Reino Unido, UN Doc. CCPR / C / GBR / CO / 7, 17 de agosto de 2015, párr. 24, donde expresó su preocupación por la "falta de salvaguardas suficientes con respecto a la obtención de comunicaciones privadas de agencias de seguridad extranjeras y el intercambio de datos de comunicaciones personales con dichas agencias".

52. Las absurdas consecuencias del razonamiento que lleva a cabo la mayoría son aún más patentes en el siguiente ejemplo: si un londinense envía un mensaje mediante Twitter a otro londinense, y esa comunicación se transmite a través de un servidor en los Estados Unidos, el Tribunal acepta que la interceptación por parte de la Sede General de Comunicaciones del Gobierno (GCHQ) de ese mensaje y los datos relacionados con las comunicaciones, cuando salgan del Reino Unido en un cable con destino a los Estados Unidos, merecen la garantía de autorización independiente. Pero si la NSA intercepta ese mismo mensaje en el otro extremo del mismo cable y luego le da una copia a la GCHQ, o los datos relacionados con las comunicaciones que le conciernen, la garantía de independencia no se aplica a la autorización. Es completamente arbitrario que haya diferentes protecciones legales para los mismos datos basados únicamente en la ubicación accidental de quien llevó a cabo la interceptación inicial. La ausencia de un sistema legal de salvaguardas para el uso de datos interceptados por un país extranjero que sea igualmente protector que el que se aplica para interceptar los datos recopilados internamente en el país, significa que la ley del Reino Unido es insuficiente para proteger contra la arbitrariedad y el abuso[160].

53. Además, de conformidad con el párrafo 12.6 del Código IC, las secciones 15 y 16 de la RIPA no son de aplicación a la totalidad del material recibido de los servicios de inteligencia extranjeros que pudieran ser el resultado de una interceptación masiva, sino solo al material interceptado solicitado o "cuando el material se identifique a sí mismo como el producto de la interceptación", lo que conlleva que el despliegue de las garantías internas del Estado receptor (el Reino Unido) dependa de una decisión de los servicios de inteligencia extranjeros.

54. La descripción del intercambio de material de forma masiva con otras partes estaría incompleta sin hacer referencia a otra característica digna de mención. Debe añadirse que el párrafo 7.3 del Código IC permitía la divulgación de material interceptado a otras partes basada en la mera conveniencia para el servicio, un criterio sorprendentemente simplista. El "principio de necesidad de saber"[161] es el opuesto lógico del test de necesidad y de proporcionalidad: el principio de que solo una parte del material interceptado puede ser divulgada ya que el receptor lo necesita es la antítesis de aquel test. El uso de este poder de divulgación no está sujeto a un umbral legal objetivo, sino meramente guiado, y posiblemente desviado, por el fin perseguido. Así, las consideraciones puramente oportunistas prevalecieron sobre la evaluación de la necesidad y la proporcionalidad de la interferencia con los derechos del sujeto de la interceptación constituida por la divulgación del material interceptado a otras partes. En palabras simples, la comunicación del individuo se trata como una posesión del Estado, una mercancía que el Estado puede compartir con otras partes a su discreción para "ver si el pajar contiene una aguja"[162].

C. Interceptación masiva de datos relacionados con las comunicaciones.

55. Por último, la sección 16 (2) de la RIPA no se aplicaba a la interceptación masiva de datos relacionados con las comunicaciones, lo que significaba que cualquier analista podía utilizar un selector fuerte referible a un individuo que se conocía que se encontraba en las Islas Británicas sin certificación previa de la Secretaría de Estado y,

[160] Esto es exactamente lo que pide la Comisión de Venecia (véase el apartado 201 de esta Sentencia).
[161] Párrafo 7.3 del Código IC (ver párrafos 96 y 390 de la presente Sentencia).
[162] Alegaciones del Gobierno demandado durante la vista ante la Gran Sala de 10 de julio de 2019.

peor aún, los datos interceptados podían almacenarse durante "varios meses", siempre y cuando fuera necesario para descubrir "incógnitas desconocidas"[163]. En términos prácticos, la interceptación y el tratamiento de los datos relacionados con las comunicaciones se limitaban únicamente por la capacidad de almacenamiento de los servicios interceptores. De hecho, realmente la RIPA no consagra un poder de recopilación de inteligencia extranjera, porque el desarrollo tecnológico lo ha transformado en un poder de vigilancia interno, y es por eso que el Gobierno ahora pretende que las salvaguardas de las Islas Británicas previstas en la sección 16 de la RIPA no sean "necesarias" para el cumplimiento de Convenio[164].

56. El argumento de viabilidad del Gobierno[165] tampoco me convence. Es perfectamente factible que un juez evalúe, a su debido tiempo, la necesidad y la proporcionalidad de una solicitud de autorización relativa a los datos relacionados con las comunicaciones de un individuo en todos los casos, sin ningún tipo de riesgo de socavar su uso[166]. Si este proceso de autorización puede ser establecido cuando se focaliza en periodistas y otros profesionales cuyos datos relacionados con las comunicaciones son legalmente privilegiados, tal como acepta el Tribunal[167]¿por qué no se puede establecer para los datos relacionados con las comunicaciones del mortal común? Estos sistemas de aprobación que operan a escala son perfectamente posibles. La cuestión es que las interferencias a gran escala con la privacidad requieren un sistema de salvaguardas a gran escala.

57. Independientemente de su grado de intromisión, tanto dentro como fuera de las Islas Británicas, la tolerancia del Tribunal con estas prácticas es incomprensible, teniendo en cuenta que la sección 16 (2) es considerada por el propio Tribunal, como "la principal salvaguarda legal que circunscribe el proceso de selección del material interceptado para su examen"[168].

D. Conclusión preliminar

58. En conclusión, el hecho de que el alcance de la actividad de vigilancia considerada en los asuntos *Weber y Saravia* (2006) y *Liberty y otros* (2008) fuera mucho más limitado de lo que es hoy no debería haber llevado al Tribunal a ser menos exigente en

[163] Párrafos 422 a 423 de la presente Sentencia.

[164] Véanse las alegaciones del Gobierno demandado durante vista ante la Gran Sala el 10 de julio de 2019. De esta manera, la autoridad de interceptación podía obtener, mediante una orden de interceptación masiva, el contenido que debería haber obtenido a través de una orden individual y dirigida bajo la sección 8, y por lo tanto podía eludir la sentencia de este Tribunal en *Kennedy c. Reino Unido*, antes citada.

[165] Párrafo 420 de la presente Sentencia.

[166] Mi juicio se basa en mi propia experiencia como juez de un tribunal penal en casos penales complejos, donde la policía a menudo solicitaba la interceptación de grandes cantidades de datos relacionados con las comunicaciones.

[167] Párrafo 450 de la presente Sentencia.

[168] Compare y contraste §§ 420 y 421. Note que en § 420 el lenguaje es "la principal salvaguarda legal", pero en § 421 se reduce a "una salvaguarda importante". El lenguaje impreciso en § 421 es desconcertante, pero aún más inquietante es la falta de sustancia. La mera manipulación del idioma es fundamental para la diferente ponderación de las "preocupaciones" planteadas en § 381 y 382 en el campo de la interceptación masiva de datos relacionados con las comunicaciones. La guinda del pastel es evidentemente la "evaluación general", que permite al Tribunal alcanzar cualquier resultado que se desee (ver mi análisis de este Criterio de "justicia general" en mi voto particular a *Muhammad y Muhammad contra Rumania* [GC], núm. 80982/12, 15 de octubre de 2020, y *Murtazaliyeva c. Rusia* [GC], Núm. 36658/05, 18 de diciembre de 2018).

cuanto al nivel de protección del derecho a la privacidad requerido. El aumento exponencial de la actividad de vigilancia en la última década y la protesta pública que ha desatado justifica una supervisión más estricta de las actividades de las agencias de inteligencia, con el fin de preservar la democracia y defender el estado de derecho. No al contrario. Cuando el riesgo de abuso estatal aumenta, las salvaguardas del Convenio y la legislación nacional correspondiente deberían aumentar también las garantías, no disminuirlas[169]. En otras palabras, los estándares actuales de protección deberían ser más exigentes que los de 2006 o 2008. Esto es exactamente lo contrario de lo que ha previsto esta sentencia. En la misma, el Tribunal ha sucumbido al *hecho consumado* de la interceptación masiva, aceptando peligrosamente que si es útil debería ser permisible. No es lo mismo utilidad que necesidad y proporcionalidad en una sociedad democrática. Como dijo el juez Brandeis en el asunto *Olmstead c. Estados Unidos*[170], "[E]s también irrelevante que la interceptación [de escuchas telefónicas] contribuyera a la aplicación de la ley. La experiencia debe enseñarnos a estar más en guardia para proteger la libertad cuando los fines del gobierno son benéficos".

V. CONCLUSIÓN

59. Esta sentencia altera el equilibrio existente en Europa entre el derecho al respeto de la vida privada y los intereses de seguridad pública, pues admite la vigilancia no selectiva del contenido de las comunicaciones y datos relacionados en las comunicaciones, y lo que es peor, el intercambio de datos con terceros países que no tienen la protección del Consejo de Europa. Esta conclusión está justificada en vista del rechazo perentorio del TJUE al acceso a una base generalizada con el contenido de las comunicaciones electrónicas[171], su reticencia manifiesta con respecto a la retención general e indiscriminada de datos del tráfico y de ubicación[172] y su limitación a los intercambios de datos con servicios de inteligencia extranjeros que no garantizan un nivel de protección esencialmente equivalente al garantizado por la Carta de los Derechos Fundamentales[173]. Sobre estos tres aspectos, el Tribunal de Estrasburgo va por detrás del de Tribunal de Luxemburgo, que sigue siendo el faro de los derechos de privacidad en Europa.

60. Para bien o para mal, y considero que más para mal que para bien, con la presente sentencia, el Tribunal de Estrasburgo acaban de abrir las puertas a un "Gran Hermano" electrónico en Europa. Si esta es la nueva normalidad que mis colegas doctos de la mayoría quieren para Europa, no puedo unirme a ellos, y esto lo digo con el corazón desencantado y con la misma consternación que aquella que emana del *Miserere mei, Deus* de Gregorio Allegri.

VOTO CONJUNTO PARCIALMENTE DISIDENTE DE LOS JUECES LEMMENS, VEHABOVIĆ, RANZONI Y BOŠNJAK

[169] *Szábo y Vissy*, antes citada, § 70: "Es necesario mejorar las garantías exigidas por la jurisprudencia del Convenio sobre intercepciones para abordar la cuestión de tales prácticas de vigilancia". Asimismo, la Resolución PACE 2045 (2015) insistió en la necesidad de supervisión reforzada de la vigilancia masiva
[170] 277 US 438.
[171] Párrafo 226 de la presente Sentencia.
[172] Párrafos 211, 217, 239-241 de la presente Sentencia.
[173] Párrafo 234 de la presente Sentencia.

1. Mostramos nuestra conformidad con la presente sentencia, con excepción de la valoración acerca de la recepción por parte de las autoridades del estado demandado de material interceptado por servicios de inteligencia extranjeros, de conformidad con los artículos 8 y 10 del Convenio (ver puntos 3 y 5 de la sentencia).

2. En la presente sentencia -como también se prevé en la sentencia de hoy *Centrum förrättvisa contra Suecia* (núm. 35252/08) - para los regímenes de interceptación masiva, la Gran Sala ha establecido un sistema de salvaguardas efectivas "de extremo a extremo", con tres pilares o piedras angulares principales, con el fin de minimizar el riesgo de que se abuse de tal poder. Estos pilares fundamentales son: (1) la autorización previa de interceptación masiva, cuando el objeto y alcance de la operación estén siendo definidos, por un organismo independiente del ejecutivo; (2) la autorización interna previa cuando son empleados selectores fuertes vinculados a individuos identificables y (3) la supervisión de la operación por una autoridad independiente junto con una revisión *ex post facto* efectiva por parte de un organismo independiente del ejecutivo (véanse párrafos 350 a 359 de la sentencia).

3. Las mismas salvaguardas "de extremo a extremo" establecidas para el régimen de interceptación masiva también deben aplicarse a un régimen en el que las autoridades no interceptan ellas mismas las comunicaciones transfronterizas y datos de las comunicaciones, sino que piden a los servicios de inteligencia extranjeros que intercepten dichos datos o les transmitan datos ya interceptados. Sin embargo, mientras al recibir el material interceptado, las garantías para su examen, uso y almacenamiento, su ulterior transmisión, y su borrado y destrucción, son igualmente aplicables (ver apartado 498 de la sentencia), el primer pilar, que es la autorización previa independiente, desaparece por completo en opinión de la mayoría. Su razonamiento al respecto no nos convence. ¿Por qué debería hacerse una distinción de acuerdo con la forma en que las autoridades acceden a la posesión de los datos interceptados, ya sea que hayan interceptado los datos por sí mismas o los haya interceptado una autoridad extranjera? Por lo tanto, en nuestra opinión, también en lo que respecta al primer pilar, deben aplicarse las mismas salvaguardas establecidas para la interceptación masiva.

4. Suscribimos plenamente la evaluación del Tribunal en los párrafos 496 y 497 de la sentencia, en particular respecto a que una injerencia en el artículo 8 radica en la propia solicitud inicial a las autoridades extranjeras, y que la protección otorgada por el Convenio sería anulada si los Estados pudieran eludir sus obligaciones del Convenio solicitando tales datos a Estados no contratantes. Los Estados miembros deben, por tanto, disponer de información clara y reglas detalladas que brinden garantías efectivas contra el uso de sus poderes para eludir la legislación nacional y / o sus obligaciones en virtud del Convenio.

5. Donde nos apartamos respetuosamente de la mayoría es en la cuestión de en qué consisten las "garantías efectivas".

6. La mayoría se refiere en primer lugar al hecho de que las solicitudes se basaron en órdenes ya autorizadas por el Secretario de Estado o explícitamente aprobadas por él (ver párrafo 505 de la sentencia). Sin embargo, argumentan que el Secretario de Estado no es independiente del ejecutivo y, a este respecto, el régimen que rige la recepción de inteligencia de los servicios de inteligencia extranjeros se ve afectada por la misma deficiencia que el régimen de interceptación masiva (ver párrafo 377 de la sentencia).

7. En segundo lugar, la mayoría parece suponer que una ley nacional que establece que no debe haber ninguna elusión es, en sí misma, una salvaguarda (ver apartado 506 de la sentencia). Respetuosamente discrepamos. Como ya se señaló, por ejemplo, en el voto particular del Juez Ranzoni en *Breyer c. Alemania* (núm. 50001/12, 30 de enero de 2020), el derecho interno solo prevé la base jurídica que determina la legalidad de la interferencia: no constituye, además y por sí misma, una salvaguarda para proteger a la persona de la aplicación de la legislación nacional por parte de las autoridades nacionales de manera arbitraria y el abuso de sus poderes legales. Dicha protección debe ir más allá de las normas legales, en particular cuando esas normas y poderes se expresan en términos amplios.

8. En otras palabras, una norma legal que prohíbe la elusión o el mal uso no puede ser al mismo tiempo una salvaguarda para que eso no suceda. Una salvaguarda eficaz supone disponer de un mecanismo capaz de asegurar la correcta aplicación de esa misma regla. Sin embargo, falta una salvaguarda de ese tipo con respecto a las solicitudes de datos interceptados y transmitidos por servicios de inteligencia extranjeros. En nuestra opinión, como en la mayor parte del régimen de interceptación, el primer pilar dentro de las salvaguardas "de extremo a extremo" debería aplicarse de manera similar. En consecuencia, cualquier solicitud de este tipo debe estar sujeta a la autorización previa de un organismo independiente capaz de evaluar si es necesario y proporcionado respecto del objetivo perseguido (véanse los apartados 350 y 351 de la sentencia), y de asegurar que esta facultad no sea utilizada para eludir la legislación nacional y / o las obligaciones del Estado en virtud del Convenio.

9. Por estas razones, hemos votado en contra de la conclusión alcanzada por el Tribunal de que no se ha violado el artículo 8 del Convenio con respecto a la recepción de información por parte de servicios de inteligencia extranjeros.

10. Dado que la mayoría concluye que el régimen de intercambio de información no vulnera lo establecido en el artículo 10 del Convenio, por las mismas razones que los llevó a concluir que no se había producido una violación de lo dispuesto en el artículo 8 (ver párrafo 516 de la sentencia), estamos igualmente en desacuerdo con la conclusión alcanzada en relación a la vulneración del artículo 10.

ANEXO

Lista de demandantes

Núm. de demanda	Demandante
58170/13	Big Brother Watch
58170/13	English PEN
58170/13	Open Rights Group
58170/13	Dña. Constanze Kurz
62322/14	Oficina de Periodismo de Investigación
62322/14	Dña. Alicia Ross
24960/15	Amnistía Internacional
24960/15	Bytes For All
24960/15	Consejo Nacional de Libertades Civiles (“Liberty”)
24960/15	Privacidad Internacional
24960/15	Unión Americana de Libertades Civiles
24960/15	Asociación canadiense de Libertades Civiles
24960/15	Iniciativa Egipcia por los Derechos Personales
24960/15	Unión Húngara de Libertades Civiles
24960/15	Consejo Irlandés para las Libertades Civiles
24960/15	Centro de Recursos Legales