Derecho a la privacidad. Intercepción de comunicaciones.

TEDH, *Case of Big Brother Watch and others vs. The United Kingdom*, 13 de septiembre de 2018 y TEDH, *Case of Catt vs. The United Kingdom*, 24 de enero de 2019. Las resoluciones del Tribunal Europeo de Derechos Humanos concernientes a privacidad ante la posible consumación del Brexit

Por Damián Loreti[1]

En dos fallos recientes contra el Reino Unido, el Tribunal Europeo de Derechos Humanos (TEDH o Tribunal de Estrasburgo) se ha pronunciado respecto a la interpretación de las políticas de recolección, retención y cesión de datos personales a terceros. Los casos son conocidos como "Big Brother"[2] y "Catt".[3]

Los efectos de las decisiones del Tribunal de Estrasburgo adquieren una particular relevancia en la medida en que el Gobierno británico ha intentado exponer que el Brexit es una oportunidad para abandonar la controvertida Carta de Derechos Fundamentales. Argumenta que el tratado representa una valla contra la eficacia en la lucha contra el crimen y el terrorismo, especialmente a causa de la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE, ubicado en la ciudad de Luxemburgo).

1 Abogado (UBA). Doctor en Ciencias de la Información (Universidad Complutense de Madrid). Profesor de grado y posgrado en Derecho a la Información y Libertad de Expresión desde 1988. Es secretario del Centro de Estudios Legales y Sociales (CELS). Ha sido perito ante la Corte Interamericana de Derechos Humanos y desde 1990 asesora a organizaciones sindicales y de medios comunitarios nacionales y regionales en materia de libertad de expresión y radiodifusión.

2 TEDH, *Case of Big Brother Watch and others v. The United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15), 13 de septiembre de 2018.

3 TEDH, *Case of Catt v. The United Kingdom* (Application no. 43514/15), 24 de enero de 2019.

Las pautas seguidas en las negociaciones con la UE de acuerdo al Libro Blanco presentado al Parlamento Británico por la Primera Ministra, Theresa May,[4] se dividen en doce secciones, las cuales abordan las prioridades del Reino Unido:

1. proporcionar seguridad jurídica y claridad para las empresas, el sector público y el público en general;

2. tomar el control de la aplicación de las propias leyes británicas sin influencia externa y poner fin a la jurisdicción del Tribunal de Justicia de la Unión Europea en el Reino Unido;

3. reforzar la unidad entre las cuatro partes del Reino Unido;

4. proteger los lazos históricos con Irlanda manteniendo la zona común de tránsito o "Common Travel Area";

5. controlar la inmigración, incluyendo la relativa a los nacionales de la UE que llegan al Reino Unido;

6. reforzar en la medida de lo posible los derechos de los ciudadanos de la UE que ya se encuentren en el Reino Unido y de los nacionales británicos que se encuentren en los otros Estados miembros;

7. proteger los derechos de los trabajadores británicos;

8. asegurar el libre comercio con los mercados europeos sin pertenecer al Mercado Único;

9. negociar nuevos acuerdos comerciales bilaterales con otros países;

10. asegurar que el Reino Unido siga siendo el mejor lugar para la ciencia y la innovación;

11. cooperar en la lucha contra el crimen y el terrorismo; y

12. proceder a una salida tranquila y ordenada de la UE.

Considerando los puntos 2 y 11, las resoluciones del TEDH en materia de compatibilidad de las reglas de colección de datos y sistemas de vigilancia electrónica serán de importancia capital. Es en este contexto que analizaremos los mencionados casos recientes.

Ya desde hace algunos años,[5] el Tribunal Europeo de Derechos Humanos ha venido resolviendo casos sobre regulaciones y decisiones de autoridades administrativas, independientes y/o judiciales de países europeos sobre temas de espionaje y vigilancia electrónica y con énfasis en algunos como consecuencia del llamado "caso Snowden".

4 "The United Kingdom's exit from and partnership with the EU", Febrero de 2017. Recuperado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/589191/The_United_Kingdoms_exit_from_and_partnership_with_the_EU_Web.pdf

5 Entre otros, TEDH, *Centrum För Rättvisa v. Suecia*, 19 de junio de 2018 y *Ben Faiza v. Francia*, 8 de febrero de 2018.

Ello no fue fruto de la casualidad sino del rechazo que produjeron –sobre todo en las organizaciones de derechos humanos y protectoras de la privacidad o de la libertad de expresión– las medidas desencadenadas a partir de la denominada "lucha contra el terrorismo", las cuales, organizada y metódicamente, fueron impugnadas en diferentes tribunales y ámbitos.

En este contexto, como decíamos, el TEDH resolvió en setiembre de 2018 el caso "Big Brother" y el 24 de enero de 2019 el caso "Catt".

1. Big Brother Watch and others vs. The United Kingdom

Esta primera sentencia se relaciona con una serie de regulaciones dictadas por el gobierno del Reino Unido que resultaban violatorias de las reglas y estándares de derechos humanos vinculados a la libertad de expresión y al derecho de privacidad.

Las regulaciones denunciadas ante el TEDH se encuentran agrupadas en la *Regulation of Investigatory Powers Act 2000* (RIPA en la jerga) y tienen por finalidad la interceptación masiva de las comunicaciones, la adquisición de datos de telecomunicaciones y el intercambio de comunicaciones y metadatos interceptados, entre el Reino Unido y Estados Unidos.

Los litigios, en concreto, fueron tres, presentados originalmente por separado, pero finalmente resueltos en conjunto: *Big Brother Watch* (App. N° 58170/13), *Bureau of Investigative Journalism and Alice Ross* (App. N° 62322/14) y *10 Human Rights Organisations* (App. N° 24960/15). Aun no habiendo casos de aplicación específicos, el trámite de las denuncias fue avalado a nivel europeo.

Luego de las revelaciones hechas por Edward Snowden, las organizaciones peticionantes iniciaron sus planteos entendiendo que estaban ante la existencia de operaciones de espionaje y vigilancia electrónica desarrolladas por servicios de inteligencia británicos y estadounidenses. Las cuestiones planteadas fueron tres:

- interceptación a granel de comunicaciones "externas" en virtud del párrafo 8 (4) de la RIPA, así como datos de comunicaciones conectados entre sí;

- el proceso de intercambio mediante el cual las agencias británicas recibieron datos recolectados por los Estados Unidos

- el acceso a los datos de comunicaciones cursadas bajo las reglas del capítulo II de la RIPA.

La base del planteo de las tres presentaciones giró en torno a que la legislación británica no respetaba los estándares que el TEDH había fijado en casos anteriores (en particular el precedente "Weber and Saravia vs. Germany").[6] Este aspecto del planteo resulta relevante toda vez que se trata de contraponer la ley aprobada en el Reino Unido con la jurisprudencia del TEDH.

6 App. No. 54934/00, Decision on Admissibility, 29 de junio de 2006.

Los estándares que determinan la pertinencia de las reglas de vigilancia que este sistema regional de derechos humanos no considera ilegal de por sí son conocidos también como "salvaguardas mínimas" y comprenden los siguientes puntos:

- Definición de la naturaleza de los delitos que pueden requerir o tener entidad para una orden de intercepción o intervención.

- Definición de las categorías de las personas susceptibles de tener sus teléfonos intervenidos.

- Límite a la duración de la intervención.

- Procedimiento a ser seguido para el examen, uso y almacenamiento de los datos obtenidos.

- Precauciones a ser adoptadas para el caso de comunicar los datos a otras partes o autoridades.

- Circunstancias en las que los registros pueden o deben ser destruidos junto a sus soportes materiales.

1.1 La decisión

El Tribunal, inicialmente, partió de la premisa que define que, cuando es realizada de modo indiscriminado, la interceptación masiva no está necesariamente en violación del artículo 8 de la Convención Europea de Derechos Humanos que protege el derecho de privacidad.

De hecho, sostiene el TEDH que los gobiernos pueden manejar "un amplio margen de apreciación" para resolver la naturaleza de los procesos de vigilancia que estimen apropiados para proteger su seguridad nacional en función de la regla del "test tripartito", que exige legalidad previa y precisa, fin legítimo y necesidad social imperiosa en el estado de derecho.

En la medida en que parte del planteo de los peticionantes era la ausencia de una autorización judicial previa como exigencia procesal para las prácticas de vigilancia e intercepción ante la actuación del Estado y los modos del tratamiento de datos, el Tribunal acordó que la autorización judicial era una salvaguarda importante, tal vez incluso "la mejor práctica", pero que por sí sola no era ni necesaria ni suficiente como regla formal para garantizar el cumplimiento del artículo 8 de la Convención. Es más, sostuvo que se tenía que tener en cuenta el funcionamiento real del sistema de interceptación, incluidos los "controles y balances sobre el ejercicio del poder" por parte de los distintos órganos del Estado.

En el análisis de la legislación, en concreto, el TEDH entendió que la norma era clara en cuanto a las circunstancias en las cuales se podía emitir una orden. Es decir, que cumple con el requisito de legalidad formal que se exige a todas las regulaciones que pueden afectar el ejercicio de derechos humanos. Asimismo, aceptó que las disposiciones sobre la duración y la renovación de las órdenes de interceptación, las disposiciones relativas al almacenamiento, acceso, examen y utilización de los datos interceptados, las disposiciones sobre el procedimiento a seguir para comunicar los datos interceptados a otras partes y las relativas al borrado y la destrucción del material de interceptación proporcionaban salvaguardas adecuadas contra el abuso.

Hasta allí, por los principios generales sentados, se podría asumir que la instalación de sistemas de interceptación y vigilancia no resulta incompatible con el artículo 8. Pero el TEDH resuelve, al mismo tiempo, que el diseño del sistema no es completamente compatible con las reglas de derechos humanos y que exhibe algunas debilidades.

Por ejemplo, el Tribunal considera grave la inexistencia de una normativa que asiente la obligación estatal de dar a publicidad los criterios de selección de qué tipo de identificación podría usar para la vigilancia masiva (datos de correo, perfiles de redes sociales, usuarios de aplicaciones, etc.), o de los criterios empleados para las búsquedas en general. El TEDH entendió que la definición de tales parámetros, así como respecto de quienes serían los operadores de tales actividades en concreto, debía estar sujeta a la expedición de una orden previa de supervisión por parte de un órgano independiente.

Las revisiones posteriores de control –dijo el Tribunal– no son "suficientemente robustas para proporcionar garantías adecuadas contra el abuso".

Una especial consideración estuvo dedicada a los "datos de las comunicaciones" (no el contenido de los mensajes sino los metadatos) que el gobierno no consideraba sensibles.

El TEDH entendió que el contenido de una comunicación electrónica podría estar encriptado y, aunque fuera descifrado, podría no revelar nada de nada sobre el remitente o el destinatario.

Los datos de comunicaciones conexos –o metadatos–, en tanto, sí podrían revelar las identidades y la ubicación geográfica del remitente y del destinatario y el equipo a través del cual se lleva a cabo la comunicación.

Aclaramos nosotros que con la intercepción "a granel" –bulk– el grado de intrusión se magnifica, ya que los patrones que emergen del tratamiento de los datos podrían ser capaces de pintar una imagen íntima de una persona a través del mapeo de redes sociales, localización, seguimiento de navegación por Internet, diseño de patrones de comunicación y análisis de la asiduidad de intercambios entre ciertas personas.

Desde la perspectiva del TEDH también constituye una violación a las reglas de privacidad protegidas por el artículo 8.

El Tribunal evaluó asimismo la naturaleza de la actividad de transferencias y cesiones de datos internacionales, cuestión sobre la que no existían precedentes.

Como ya hemos dicho, le preocupaba no solo la intervención sobre contenidos, sino también sobre los datos de las comunicaciones. Es decir, la recepción del material interceptado y el posterior almacenamiento de datos y metadatos, así como su examen y uso posterior por los servicios de inteligencia.

Al respecto, el TEDH apuntó:

> Con cualquier regulación que prevea la adquisición de material de vigilancia, el régimen para la obtención de dicho material de los gobiernos extranjeros debe ser conforme a la ley […] y debe ser proporcional al fin legítimo perseguido, y deben existir salvaguardas adecuadas y eficaces contra el abuso […] En particular, los procedimientos para supervisar el ordenamiento y aplicación de las medidas en cuestión deben ser tales que mantengan la "injerencia" en lo que es "necesario en una sociedad democrática".

En el mismo sentido manifestó su preocupación por el hecho de que los Estados utilizaran el intercambio de inteligencia "como medio para eludir los controles".

En cuanto a otras peticiones vinculadas con la incompatibilidad de las reglas británicas con los principios y estándares protectorios de la libertad de expresión, nos parece relevante la cuestión de las posibles intromisiones sobre material confidencial que formara parte de investigaciones periodísticas, a partir del funcionamiento de los regímenes de la sección 8 (4) y del capítulo II de la RIPA.

Respecto de este punto, el TEDH no consideraba antes, ni lo hizo ahora, al secreto periodístico como necesariamente inviolable.

En síntesis, la intercepción "a granel" viola el artículo 8 de la Convención Europea porque existió insuficiente control y supervisión en la elección de portadores o filtros para la detección, búsqueda y selección de las comunicaciones interceptadas para su análisis, además de que las salvaguardas que se utilizaban para la selección de los "metadatos" eran inadecuadas.

Para el caso concreto, entonces, el régimen de intercepción en teoría no es violatorio de la Convención, pero que los estándares de aplicación deberán cumplimentar las garantías que fijó el fallo al cuestionar la ley británica por la falta de requisitos específicos para limitar el poder de los servicios de inteligencia en la búsqueda de material periodístico o de otro carácter confidencial (por ejemplo, utilizando la dirección de correo electrónico de un periodista como criterio de selección).

También señaló como problemática la ausencia de exigencias para los analistas de información para tomar en cuenta si un determinado material está o puede estar vinculado con actividades periodísticas, lo cual involucra una violación del artículo 10 que protege la libertad de acceder y divulgar informaciones e ideas.

Con todos estos señalamientos, pareciera que la decisión se vio influida por "la amenaza del terrorismo internacional" y la naturaleza global de las redes terroristas que requieren un intenso flujo de información.

Pero el TEDH estimó al respecto que este flujo de información "estaba incrustado en un contexto legislativo que proporcionaba salvaguardas considerables contra los abusos", de modo que "la interferencia resultante era la necesaria en una sociedad democrática".

2. Catt vs. The United Kingdom

A poco de la sentencia "Big Brother Watch", el TEDH intervino nuevamente en un caso originado en el Reino Unido para analizar la compatibilidad de las reglas de colección, retención y uso posterior de datos personales por parte de las autoridades británicas.

En esta ocasión no se trató de un análisis de reglas estructurales del sistema de alcance general, sino que el Tribunal analizó una serie de situaciones específicas de aplicación padecidas por una persona física, el demandante John Oldroyd Catt.

Catt ha sido un activista del movimiento pacifista desde 1948 y ha participado en gran cantidad de manifestaciones públicas. En 2005 empezó a participar en manifestaciones organizadas por la campaña Smash EDO, cuyo objetivo estaba destinado a lograr el cierre de las actividades de EDO MBM Technology Ltd., empresa dedicada a la fabricación de armamentos en el Reino Unido.

En varias movilizaciones se generaron disturbios y acciones violentas que fueron reprimidas por la policía. El demandante fue arrestado dos veces en oportunidad de manifestaciones públicas de Smash Edo que obstruyeron autopistas, pero nunca tuvo sanciones ni condenas por tales hechos.

En marzo de 2010 Catt hizo un pedido de acceso a la información a la Policía, por aplicación de la Ley de Protección de Datos de 1998, a fin de requerir la información relacionada a su persona que obrara en poder de la fuerza de seguridad. Se le comunicó que existían sesenta y seis entradas referidas a otras personas que incidentalmente lo mencionaban. Todos con relación a hechos ocurridos entre marzo de 2005 y octubre de 2009.

Los datos mantenidos por la policía se encontraban en una base de datos conocida como "Base de datos del Extremismo".

La gestión de dicha base estaba a cargo de la National Public Order Intelligence Unit de la Policía británica (NPOIU). Si bien la mayoría de los registros estaban ligados a las movilizaciones en contra de EDO, había otros vinculadas a temáticas diferentes y que toman relevancia en función de la protección de datos sensibles.

Por ejemplo, su asistencia al Congreso de la Confederación de Sindicatos Nacionales, una movilización del Partido Laborista, una manifestación pro-Gaza y otra de protesta contra las reformas laborales promovidas por el gobierno británico en septiembre de 2009. También había fotos del demandante tomadas en 2007 en una de las tantas actividades públicas.

Con esta información constatada, Catt requirió la eliminación de las constancias a la autoridad policial, lo cual fue denegado sin explicación. En noviembre de 2010 inició un procedimiento judicial contra esta negativa. El objeto de la demanda era obtener una resolución que sostuviera que la retención de los datos obtenidos no era necesaria en los términos del estándar del artículo 8.2 de la Convención.

En este contexto, en 2012, una autoridad independiente, la HM Inspectorate of Constabulary, hizo un reporte relativo a operaciones encubiertas de la Policía para obtener datos de inteligencia de movilizaciones de protesta. Este reporte concluía en que la información estaba innecesariamente retenida en archivos y registros policiales. Como consecuencia del informe se borraron y eliminaron archivos y registros. De aquellos en los que se mencionaba a Catt solo quedaron dos.

En el marco del procedimiento judicial, el demandante requirió a la policía tener acceso a sus registros. El pedido fue rechazado diciendo que no se los darían por "obvias razones". La respuesta oficial fue más allá: "Una base de datos de inteligencia pierde su eficacia si no se la mantiene confidencial".

También como resultado de la acción judicial se requirió al gobierno que informara si existían datos adicionales. De este pedido surgieron cuatro registros más ligados al desarrollo de acciones judiciales por terceras personas. Dos de ellos fueron eliminados más tarde, pero los restantes permanecieron.

Presentada así, la causa por la eliminación de los registros de Catt todavía existentes en poder la Policía y otras agencias estatales como la Association of Chief Police Officers (ACPO) fue rechazada por la instancia inferior, pero la Cámara de los Lores revocó ese fallo e hizo lugar a la petición. No obstante, el Comisionado de Policía y la ACPO interpusieron sendos recursos de apelación y el caso llegó a la Suprema Corte.

El máximo tribunal británico señaló en términos doctrinales generales que la recolección, tratamiento y retención indiscriminada de datos personales implica una injerencia no habilitada por el artículo 8.2 de la Convención Europea, salvo que se justifique claramente en aras del interés público.

Entendió así que, en el caso, la recolección y el procesamiento eran legales a la luz del articulo 8 y que –en el caso– la discusión podría discurrir sobre la presencia de la necesidad social imperiosa en la retención sine die de los datos y registros.

Sin embargo, la mayoría de los integrantes del tribunal entendieron que no se trataba de datos sensibles sino de registros obtenidos de terceros y de presencias en manifestaciones públicas. Y que, como los datos no quedaron en registros nominados específicamente, no existía violación a las reglas aplicables, en tanto la retención de los mismos no importaba la asignación de responsabilidades penales ni consideraciones estigmatizantes.

Al finalizar el procedimiento doméstico, de los sesenta y seis registros solo quedaron dos pendientes y cuatro menciones en relación a terceros.

En este contexto se presenta la acción de Catt ante el TEDH. Nos adelantamos a señalar que aun habiendo sido puesta en análisis la compatibilidad del marco legal y reglamentario sobre la cuestión, la resolución final del Tribunal Europeo se apoyó en la falta de cumplimiento del estándar de necesidad social imperiosa.

También es oportuno indicar, en virtud de las consideraciones iniciales volcadas en el presente, que el TEDH decide en forma contraria a los estándares del TJUE, que previamente había admitido como justificable la recolección indiscriminada de datos personales.

2.1 La posición del TEDH

El demandante sostuvo en su requerimiento que la recolección sistemática, así como la retención de sus datos en una base de búsqueda, violaban sus derechos a la luz del artículo 8 de la Convención.

Como en casos anteriores, el TEDH consideró que la mera acumulación de datos y su tratamiento posterior pueden implicar una interferencia con los derechos mencionados.

En este caso, no había controversia respecto a que se atribuía lo actuado a la protección de un interés legítimo, tal como prevenir desórdenes graves y salvaguardar los derechos de terceros.

Al respecto, se debe tener en cuenta que la aplicación del concepto de "domestic extremist", de acuerdo a las autoridades, no respondía a una definición estricta establecida por la ley, sino que se trataba de "un descriptor generalmente usado por los servicios policiales para señalar la actividad de individuos o grupos que llevan adelante actos criminales o acciones directas para fomentar sus campañas de protesta por fuera del proceso democrático". Este punto, sin duda, debió haber sido impugnado por la vaguedad de la figura utilizada.

Sentadas estas premisas y salvedades, diremos que el demandante planteó ante el TEDH que la "recolección sistemática", así como la "retención" de información respecto a su persona en una base de datos de tratamiento y búsqueda, violaban sus derechos establecidos en el artículo 8 de la Convención.

A fin de poner en juego la interpretación correcta de los alcances del artículo 8, se tomaron en cuenta los textos del Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108) de 1981, el Protocolo adicional a este Convenio, aprobado en el año 2001[7] y el Protocolo modificatorio que se encuentra abierto a la firma de los Estados desde octubre de 2018.[8]

En particular, el artículo 8 de este último Protocolo (que modifica la redacción original del art. 6) resultó fundamental para el TEDH a la hora de fijar el estándar pertinente en cuanto al tratamiento de datos personales,[9] en sintonía con otras declaraciones y acuerdos europeos.

7 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.

8 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

9 "Artículo 8: El texto del Artículo 6 de la Convención será reemplazado por el siguiente:
1. El tratamiento de:
- datos genéticos;
- datos personales relativos a delitos, procedimientos penales y condenas, y medidas de seguridad conexas;
- datos biométricos que identifiquen de forma única a una persona;
- los datos personales relativos a la información que revelen en relación con el origen racial o étnico, las opiniones políticas, la afiliación sindical, las creencias religiosas o de otra índole, la salud o la vida sexual, sólo se permitirán cuando se establezcan las garantías adecuadas en la ley, que complementen las del presente Convenio.
2. Dichas garantías protegerán contra los riesgos que el tratamiento de datos sensibles pueda presentar para los intereses, derechos y libertades fundamentales del interesado, en particular un riesgo de discriminación". Traducción propia.

En forma separada, el Tribunal también abordó el caso a la luz de los instrumentos de la Unión, en especial la Directiva de protección de datos personales de 1995 y su reforma de 2016 que resultó en la aprobación del nuevo Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (GDPR por sus siglas en inglés).

El TEDH considera aplicables los principios generales expresados en esa regulación, pero también valora especialmente las definiciones contenidas en un documento que fue aprobado y entró en vigencia en el mismo momento que el Reglamento como parte de la legislación comunitaria: la Directiva 2016/680, conocida como "Law Enforcement Directive" (LED).

La LED otorga mayores prerrogativas a los Estados para el procesamiento de datos cuando se trata del cumplimiento de funciones relativas a la seguridad y la política criminal. El TEDH retoma de esta Directiva la definición de "procesamiento de datos" y, en especial, las condiciones para el procesamiento de "categorías especiales de datos" por parte de agencias estatales.

Así, mientras el Reglamento general prevé en su artículo 9 que el tratamiento de los datos considerados de categorías especiales debe estar prohibido salvo excepciones muy específicas, el artículo 10 de la LED sostiene lo siguiente:

> El tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física solo se permitirá cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado y únicamente cuando: a) lo autorice el Derecho de la Unión o del Estado miembro; b) sea necesario para proteger los intereses vitales del interesado o de otra persona física; c) dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

Bajo este marco, el TEDH no encuentra controversia respecto a la existencia de fin legítimo y, por lo tanto, no cuestiona de manera directa la recolección y procesamiento de datos.

La sentencia hará hincapié, en cambio, en el reconocimiento por parte del Gobierno británico respecto de la extensión temporal de la retención de los datos y su interferencia sobre los derechos de Catt. La ley británica no consideraba un máximo para la retención, pero sí un mínimo de seis años.

Luego el TEDH cuestiona, aun no habiendo sido introducida la cuestión como un agravio específico, aunque sí como un argumento de la denuncia, la vaguedad de la definición de "extremismo doméstico" por su ambigüedad sobre el criterio que deja a la policía gobernar la recolección de los datos y que el resultado de ello es un sistema inadmisible de valoración "caso por caso".

También remarca la sentencia la carencia de un fundamento legal claro y coherente para la administración de las bases de datos a fin de prevenir situaciones de arbitrariedad.

Finalmente, el fallo analiza la presencia de "necesidad social imperiosa" –aun cuando ya se verificó la ausencia del requisito de legalidad previa, formal y precisa–.

Asume, entonces, la importancia de verificar la proporcionalidad de lo actuado, pese a la admisión de los márgenes de apreciación propios del Estado que la doctrina del TEDH reconoce inveteradamente.

Para ello, en primer lugar, destaca que los datos acumulados revelan opiniones políticas, están incluidos en la definición de datos sensibles o de categorías especiales y tienen un alto nivel de protección. De modo que, aun cuando el Estado sostiene que no hubo recolección sistemática de ellos, el TEDH entiende que faltó clarificación sobre el tema.

En este punto es relevante el principio que refrenda el TEDH al analizar la presencia o no de necesidad social imperiosa en la resolución del caso. Allí contradice al Estado diciendo que lo que hay que analizar no es si había "necesidad social imperiosa para la policía a fin de crear y mantener una base de datos como esa", sino si era necesario tener allí los datos del demandante, y concluye que el tribunal doméstico tenía razón dadas las actividades del grupo que eran potencialmente violentas y delictivas.

En la medida en que a Catt no se le había imputado nada, la recolección era admisible, pero no el mantenimiento en retención de los datos. Menos aún si no había ley que fijara máximos de tiempo de guarda de los mismos.

Concluye la sentencia que sería totalmente contrario a la necesidad de proteger la vida privada, en virtud del artículo 8, que el Gobierno creara una base de datos de tal manera que los datos que contiene no pudieran revisarse o editarse fácilmente y que luego utilizara esa información como justificación para negarse a eliminarla.

Palabras finales

Con la condena al Reino Unido en el caso "Catt", el TEDH reafirma lo dicho en "Big Brother" y se opone a la jurisprudencia del TJUE. Como dijimos, a pocos días del Brexit estos fallos adquieren enorme relevancia. En particular, cuando atendemos a las diferencias que surgen de los textos de los instrumentos regionales.

El contexto político global, que es explícitamente señalado en tales términos en más de una oportunidad a lo largo del texto de ambas sentencias, ha dado cuenta de la aceptación por parte del TEDH de las prácticas –sujetas a escrutinio, por cierto– de intercambio de datos entre servicios de inteligencia y compilación de información personal por razones de inteligencia de defensa y de seguridad.

En el primer caso el TEDH se autolimitó en cuanto a qué y cuánto quiso resolver, pero no discutió las bases de la reciprocidad, es decir, el intercambio de inteligencia recolectada por los servicios británicos y compartida en el extranjero.

En materia específica de libertad de expresión, este caso también trajo una novedad de importancia porque nunca antes se había abordado el tema de la vigilancia desde esta perspectiva para proteger el secreto de la fuente de información.[10]

En el segundo caso analizado, el Tribunal Europeo admitió la recolección de datos de alguien que participaba en manifestaciones públicas. Pero no admitió la retención *sine die* y sin revisión de esos datos.

El Brexit pondrá en debate el derecho supranacional europeo y su aplicación en Gran Bretaña en múltiples áreas. Salir de la UE y mantenerse en el Consejo de Europa modificará el estado del arte y dará lugar a estándares diferentes que será necesario seguir de cerca en sus implicancias sobre la libertad de expresión y el derecho a la información. Sobre todo, a tenor del contenido expresado en esta materia en el Libro Blanco, utilizado como hoja de ruta para el proceso.

10 En el precedente "Goodwin" el TEDH estableció la protección de las fuentes de información periodística como derecho comprendido en el artículo 10. Véase TEDH, *Goodwin v. The United Kingdom*, Application no. 28957/95.