Resumen: ***resolución interlocutoria que hace lugar al libramiento de oficios solicitando informes a las firmas Facebook Inc. y Microsoft, y declara la nulidad del oficio librado por el señor Fiscal, sin orden judicial, a la empresa de telefonía celular pidiendo las celdas de conexión habilitadas y su correspondiente ubicación geográfica.***

Buenos Aires, de septiembre de 2018.

ANTECEDENTES:

Ingresa la presente causa al tribunal en virtud del pedido de informes efectuado por la Fiscalía interviniente, con el objeto de recabar información de la empresa Microsoft a fin de que aporte la información de registración y conexión de la cuenta de correo electrónico xxxxxxxx@hotmail.com, para que una vez recibida la respuesta se oficie a las empresas proveedores de acceso a internet que correspondan que brinden los datos de las asignaciones de las direcciones IP que de ella resulten.

Finalmente, el señor Fiscal requirió a este tribunal, a los fines de profundizar la investigación, el libramiento de oficio a la firma Facebook Inc. a fin que informe los siguientes datos respecto del usuario de la red social Facebook con URL http://www.facebook.com/xxxxxxxx : a. Del Registro de Información Transaccional; b. Registro de direcciones IP utilizadas para el acceso, con indicación de las fechas y horas pertinentes; c. Información Registrada del usuario en cuestión; d. Abonado telefónico registrado por el usuario (págs. 17/18.).

En el mismo acto, dispuso el libramiento de oficio a la empresa de telefonía móvil a fin de que informe la titularidad, domicilio de facturación y listado de celdas de conexión habilitadas, con su correspondiente ubicada geográfica, respecto del abonado +540000000, durante el mes de octubre de 2017.

ARGUMENTOS:

I. Entiendo que cierta parte de la información de carácter personal que se requiere a las firmas Facebook y Microsoft se encuentra amparada por la garantía de la privacidad, y como tal el acceso a la misma por parte de los investigadores sin orden judicial podría redundar en una afectación a dicha

garantía (art. 17 PDCyP, art. 11.2 CADH, art. 12 DUDH, arts. 18 y 19 CN y art. 12 inc. 3º y 13.8 CCABA).

En ese sentido, de acuerdo con una interpretación amplia y dinámica del derecho a la intimidad, considero que los datos de tráfico de todo usuario de un correo electrónico y de redes sociales (registro de direcciones de IP asignadas, registro de la información transaccional)[1], registrados en las bases de datos de las empresas de telecomunicaciones, por las redes sociales o por cualquier otra plataforma digital, constituyen *"información personal almacenada"* en los términos previstos por el art. 13.8 CCABA y, en consecuencia, por imperativo constitucional, su relevamiento sólo puede ser ordenado por el juez competente.

Más específicamente, las medidas requeridas impactan sobre la protección constitucional de la vida privada o del derecho a la intimidad, a través de la afectación del derecho a la protección de los datos personales y de la autodeterminación informativa, manifestaciones del derecho a la libertad y de la autonomía individual en esta nueva era digital informática.

En palabras de la Dra. Johanna Caterina Faliero, que es una de las especialistas argentinas que con mayor detalle viene abordando la materia, "*la protección de datos personales en términos normativos ha tenido una evolución y ha evidenciado una complejización creciente en lo referente a su ámbito de aplicación y materialización. (...) Con las tecnologías de la información y la comunicación, se vela más que por el derecho clásico que concebimos de privacidad, por el denominado derecho de autodeterminación informativa*.[2]

---

1 Para obtener mayores precisiones terminológicas, consultar la "GUÍA DE BUENAS PRÁCTICAS PARA OBTENER EVIDENCIA ELECTRÓNICA EN EL EXTRANJERO", elaborado por la UNIDAD FISCAL ESPECIALIZADA EN CIBERDELINCUENCIA DIRECCIÓN GENERAL DE COOPERACIÓN REGIONAL E INTERNACIONAL, Procuración General de la Nación, año 2017, disponible en: https://www.fiscales.gob.ar/wp-content/uploads/2018/07/Gu%C3%ADa-de-Buenas-Pr%C3%A1cticas-para-Obtener-Evidencia-Electr%C3%B3nica-en-el-Extranjero.pdf . Allí se establecen tres grupos de información: básica, transaccional y de contenido. La información transaccional incluye los datos de remitente y receptor de correos electrónicos y sus direcciones IP de conexión; día y hora de las comunicaciones que se efectuaron; cantidad de datos que insumió la comunicación; sitios web visitados por el usuario.

2 FALIERO, Johanna Caterina, *"El Derecho a la información en el derecho del Consumidor y el nuevo Código Civil y Comercial -Autodeterminación informativa de los usuarios y su regimen tuitivo-"*, Pags.90/120, Publicado por el Instituto GIOJA (UBA), bajo la coordinación de Sebastián Barocelli, 2016 disponible en: https://www.eae-

Con relación a esta última cuestión, la Corte Interamericana de Derechos Humanos (en adelante, Corte IDH) reconoció que la protección a la vida privada establecida por el texto de la Convención no se agota exclusivamente en las referencias al domicilio y a la correspondencia consagradas en su texto, proponiendo entonces una interpretación dinámica de la cláusula examinada (en este sentido, Corte IDH, caso *"TRISTAN DONOSO v. Panamá"*. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia del 27 de enero de 2009. Serie C Nº 193; párr. 29).

También lo sostuvo el Tribunal Europeo de Derechos Humanos (en adelante, TEDH) al señalar que *"vida privada"* es un término amplio, no susceptible de una definición exhaustiva. Su protección no se limita a un *"círculo íntimo"* en el que el individuo desarrolle su vida personal, excluyendo de su conocimiento a cualquier otra persona externa, sino que también protege el derecho de establecer y desarrollar relaciones con otras personas y con el mundo exterior. Existe una zona de interacción de la persona con otras, incluso en un contexto público, susceptible de protección como *"vida privada"* (en este sentido, TEDH, "*PERRY c. Reino Unido"*, núm. 63737/00, párr. 36; *"PECK c. Reino Unido"*, núm. 44647/98, párr. 57 y 59, entre otros).

Si partimos de la idea conceptual tradicional de que la *"intimidad física"* supone la libertad y una carta de protección contra cualquier injerencia arbitraria del estado en la familia, el domicilio, la correspondencia, la comunicaciones y los papeles privados, es posible definir a la *"intimidad informativa"* como el derecho de cada individuo de definir cómo, quién y bajo cuáles circunstancias y condiciones se puede acceder a su información personal.

La primera sentencia en la que se reconoce a la autodeterminación informativa como un derecho fundamental del hombre fue dictada por el Tribunal Constitucional Alemán de 15 de diciembre de 1983 (sentencia de 15 de diciembre de 1983 (Ref. 1 BvR 209/83) (Fondo) Ley del Censo), en la que se reconoció que la proliferación de centros de datos y los avances

---

publishing.com/catalog/details//store/es/book/978-3-639-53666-9/di%C3%A1logo-de-fuentes-en-el-derecho-del-consumidor?locale=gb

tecnológicos han permitido producir *"una imagen total y pormenorizada de la persona"* convirtiéndose así el ciudadano en *"hombre de cristal"*.[3]

En dicho precedente se reconoció también que *"(...) la autodeterminación del individuo presupone -también en las condiciones de las técnicas modernas de tratamiento de la información- que se conceda al individuo la libertad de decisión sobre las acciones que vaya a realizar o, en caso, incluyendo la posibilidad de obrar de hecho en forma consecuente con la decisión adoptada. El que no pueda percibir con seguridad suficiente que informaciones relativas a él son conocidas en determinados sectores de su entorno social y quién de alguna manera no sea capaz de aquilatar lo que puedan saber de él sus posibles comunicantes puede verse sustancialmente cohibido en su libertad de planificar o decidir por autodeterminación. No serían compatibles con el derecho a la autodeterminación informativa un orden social y un orden jurídico que hiciese posible al primero, en el que la persona ya no pudiera saber quién, qué, cuándo y con qué motivo sabe algo sobre él. Quien se siente inseguro de si en todo momento se registran cualesquiera comportamientos divergentes y se catalogan, utilizan o transmiten permanentemente a título de información, procurará no llamar la atención con esa clase de comportamiento. Quien sepa de antemano que su participación, por ejemplo, en una reunión o en una iniciativa cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo renunciara presumiblemente a lo que supone un ejercicio de los correspondientes derechos fundamentales [artículo 8° y 9° de la Ley Fundamental (17). Esto no sólo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos".*

---

3 En dicho precedente se interpretó que resultaba lícito el recopilamiento de gran parte de los datos del censo referidos a nombre, apellidos, dirección, estado, nacionalidad, utilización de la vivienda, fuente de los medios principales de subsistencia, datos académicos y profesionales, rama de actividad, pero se declaró que resultaban ilícitos, entre otros, los preceptos relativos al cotejo de datos para ser utilizados contra las personas obligadas a suministrar esa información. Fallo disponible en versión español en *http://www.derecho-chile.cl/sentencia-de-15-de-diciembre-de-1983-del-tribunal-constitucional-federal-aleman-ley-del-censo/*

En este marco conceptual se inserta el derecho a la autodeterminación informativa, derivación de la garantía de intimidad, que prevé como regla general que cada persona tiene el derecho personal de decidir y disponer libremente sobre sus datos personales, lo que alcanza también el derecho de decidir quiénes pueden acceder a ellos.

En el orden normativo local, la Ley 25.326 de Protección de los Datos Personales que reglamenta el instituto del hábeas data previsto, en su art. 1º establece que tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero, de la Constitución Nacional.

Por su parte, en el art. 2º define como *"datos personales"* a la información de cualquier tipo referida a personas físicas o de existencia ideal; y señala expresamente que el *"titular de los datos"* es la persona cuyos datos sean objeto del tratamiento al que se refiere la ley, es decir, el *usuario*, con independencia de que esa información se encuentre en poder de un tercero.

Finalmente, en lo que aquí resulta relevante, el propio artículo define al *"tratamiento de datos"* como operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el *procesamiento de datos personales*, lo que a mi criterio incluye el relevamiento por parte de las empresas requeridas del registro de los *logs* de conexión de una cuenta o correo electrónico determinado, y de la información transaccional de la cuenta.

A pesar de que no encontramos en nuestro ordenamiento procesal una regulación procesal específica referida a esta clase de medios de prueba digitales, en el caso -además del requerimiento vinculado con el domicilio y nombre de usuario- se pretende que Facebook y Microsoft aporten el registro de la información transaccional y el registro de las direcciones de IP utilizadas por el usuario investigado para el acceso a su cuenta.

No se trata únicamente en el caso de información vinculada a los datos filiatorios (nombre y DNI) o al domicilio de los usuarios y clientes de las empresas requeridas (art. 5, inc. 2.c) de la Ley 25.326), sino que además, se pretende acceder a una serie de datos de tráfico que permitirían conocer la intimidad de los registros de transacción de una cuenta, los cuales permitirán a su vez determinar a través de las direcciones IP el/los lugar/es desde los que se realizó cada acceso o logueo del usuario, como así también –eventualmente– la/las cuenta/s con la/s que hubiere contactado.

Este es el motivo por el cual considero que nos encontramos frente a una medida que no puede ser dispuesta unilateralmente por quienes dirigen las investigaciones que en nuestro ordenamiento es el Ministerio Público Fiscal, sin intervención del único órgano constitucionalmente habilitado para permitir el acceso a ciertos ámbitos reservados.

Recientemente, en el caso *"BENEDIK c. Slovenia"* (rta. 24/04/2018), el TEDH entendió que existió una violación al derecho a la privacidad, previsto en el art. 8 de la Convención Europea de Derechos Humanos (análogo al art. 11 CADH) en un caso de distribución de imágenes con contenido de abuso sexual de personas menores de edad, en el que la Policía de Eslovenia había requerido a una empresa proveedora del servicio de internet los datos del usuario al que se le había asignado una determinada IP sin orden judicial.

Entre sus fundamentos destacó que el art. 8 de la CEDH protege el derecho de identidad y desarrollo personal, y el derecho de establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior, así como el derecho a la autodeterminación informativa, al considerar que el concepto de *"vida privada"* es un término amplio, y que por ello incluye el derecho a la privacidad con respecto al procesamiento automático de "datos personales", entendiendo por tal concepto a cualquier información relativa a un individuo identificado o identificable.

Por otra parte, explicó que la información del imputado asociada con la IP dinámica, no era información que estuviera accesible y por lo tanto no podía ser comparada a la información encontrada tradicionalmente en un directorio público. Para poder identificar a una persona a través de una IP

dinámica, la empresa prestadora del servicio debía acceder a la información almacenada concerniente a eventos de telecomunicaciones particulares, por lo que el uso de esa información, por sí sola, podía dar lugar a consideraciones sobre la vida privada.

Incluso en este precedente se avanzó hasta el punto de afirmar que si bien hay información que en principio aparece como periférica -como puede ser el nombre o el domicilio del usuario-, en ciertas situaciones, puede ser inseparablemente conectada a los restantes datos de contenido revelador, preexistentes.

Tal como lo hizo este último tribunal, para un correcto dimensionamiento de la cuestión resulta importante tomar en cuenta las disposiciones de la Convención sobre Ciberdelito (Budapest), aprobada por nuestro país mediante Ley Nº 27.411 (BO del 15/12/2017), que obliga a los Estados a llevar a cabo medidas que permitan a las autoridades combatir los crímenes relacionados con las imágenes de abuso sexual infantil, pero que también dispone que dichas medidas deben ser llevadas a cabo de conformidad con el art. 15 de la misma Convención, que establece que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en esa sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, así como que las *"condiciones y salvaguardias incluirán una* ***supervisión judicial*** *u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento"* (destacado agregado).

Ahora bien, a fin de evaluar la procedencia de la solicitud de información pretendida por el señor Fiscal, resulta pertinente recordar que en materia de privacidad la Corte Suprema de Justicia de la Nación (en adelante, CSJN), ha declarado que *"sólo por ley podrá justificarse la intromisión, siempre que medie un interés superior en resguardo de la libertad de otros, la defensa de la sociedad, las buenas costumbres o la persecusión del crimen"* (CSJN, *Fallos,* 306:1892, *"PONZETTI de BALBÍN, Indalia c. Editorial Atlántida SA"*, consid. 8º, 24/03/1994; en el mismo sentido, *"HALABI"*, H. 270, XLII, consid. 24º, entre otros).

Este estándar refleja la regulación contenida en los instrumentos internacionales de derechos humanos que forman parte de nuestra Constitución, que justamente prevén que para que toda injerencia en la vida privada debe estar prevista en la ley perseguir una finalidad legítima y resultar necesaria en una sociedad democrática (arts 30 y 32.2 CADH).

Consecuentemente, corresponde analizar si en el caso la medida probatoria solicitada resulta justificada a la luz del grado de sospecha reunido hasta el momento, y si por otra parte resulta necesaria y proporcional en atención a la gravedad del delito investigado.

Cabe recordar que el pedido de informes en este caso se articula a partir de la información proporcionada por el *National Center of Missing and Exploted Children* (NCMEC), bajo el reporte Nº 25016547 del que surge el usuario de la red Facebook con URL http://www.facebook.com/xxxxxx ID 0000000000, asociado al abonado telefónico +5400000000 y al correo electrónico xxxxxxxx@hotmail.com, y tiene por objeto recabar pruebas que permitan individualizar fehacientemente al usuario de dichas cuentas, como así también determinar el posible lugar de comisión del hecho.

En razón de ello, entiendo que se trata de una medida necesaria e indispensable para permitir el avance de la investigación, ya que en el caso no se cuenta con la dirección de IP que se corresponde específicamente con los incidentes reportados, toda vez que la misma no surge del reporte antes referido.

Por otra parte, la medida guarda correspondencia estricta con los sucesos descritos en el decreto de determinación de los hechos efectuado por la Fiscalía y entiendo que existe un grado de sospecha que permite sostener razonablemente tanto la existencia de un delito según las previsiones del art. 128 CP, como la posible participación en carácter de autor por parte del usuario investigado.

Por tales motivos, habré de autorizar el libramiento de sendos oficios a Facebook y a Microsoft, en los términos pretendidos por el señor Fiscal.

Por último, tal como lo vengo sosteniendo en numerosos precedentes, dejo sentada mi posición en cuanto a que una vez concluida la

investigación, el señor Fiscal y el Cuerpo de Investigaciones Judiciales deberán proceder a la destrucción de todos los datos y registros que no guardan trascendencia para la investigación, que obren en su poder (art. 4 inc. 7º de la Ley 25.326).

II. Ahora bien, en atención a la interpretación que he efectuado previamente respecto del alcance de la protección constitucional de la garantía de la intimidad y del derecho a la protección de datos personales y a la autodeterminación informativa, no puedo dejar de expedirme respecto al oficio cuyo libramiento dispuso el señor Fiscal sin orden judicial a la empresa de telefonía celular correspondiente al abonado +54000000000 a fin de que aporte el informe de titularidad, domicilio de facturación y *listado de celdas de conexión habilitadas con su correspondiente ubicación geográfica*.

Más allá de que considero que, en el marco de esta clase de investigaciones, los fiscales se encuentran legitimados en virtud de lo dispuesto por el art. 93, primera parte, CPPCABA, para requerir autónomamente informes referidos a los datos básicos de los usuarios investigados (datos del titular de la cuenta, como ser, nombre, país, dirección, teléfonos, y demás información registrada; dirección de correo electrónico asociada; número de teléfono celular asociado; número de tarjeta de crédito asociada; dirección IP desde la que se creó la cuenta), entiendo que es diferente el tratamiento que merece la solicitud del listado de celdas de conexión de un teléfono móvil con su correspondiente ubicación geográfica, por tratarse de una medida que se encuentra ubicada en otra categoría de mayor sensibilidad, desde la perspectiva de la privacidad.

En efecto, considero que los usuarios de los teléfonos celulares mantienen una razonable expectativa de privacidad respecto del registro de los sucesivos y constantes movimientos que van quedando capturados por las celdas de geolocalización de las antenas de las empresas prestatarias del servicio, y por lo tanto, para que puedan ser reveladas en el marco de una investigación penal, se requiere la orden de un juez.

A los fines de comprender adecuadamente las características técnicas de este tipo de medidas, conviene señalar sucintamente que el análisis de las celdas de localización permite determinar, sobre la base de la

información con que cuentan las operadoras, la ubicación de todas las terminales móviles que se activaron dentro de una "celda" (rango de cobertura geográfica de una antena) en un momento determinado.

Sobre la base de la información obtenida, se puede concluir que determinado usuario se encontraba en determinado horario, en las cercanías del lugar de los hechos; o bien, se puede determinar el presunto lugar de comisión del hecho, cuando no está suficientemente circunscripto.

Es importante destacar que los registros del posicionamiento de los usuarios quedan almacenados en los archivos de las empresas prestatarias con independencia de si el titular utiliza o no el teléfono móvil.

Más aún, se conocen ciertas técnicas de investigación llevadas a cabo en países europeos como Alemania, Holanda, Francia y España, que permiten acreditar la ubicación de personas mediante los denominados "SMS silenciosos" (*Stille SMS*), a través de los cuales las autoridades envían mensajes de texto a un destinatario cuya ubicación se pretende conocer, quien no se anoticia del mismo, no obstante lo cual el acto de comunicación queda registrado y archivado entre los datos de la operadora referidos a ese usuario.[4]

Como es notorio, se trata de una medida que tiene fuertes repercusiones desde el punto de vista de la protección de la privacidad y de la información personal que las empresas de telecomunicaciones tienen almacenada respecto de sus usuarios, únicos titulares de dichos datos, conforme los lineamientos constitucionales y normativos establecidos precedentemente.

La relevancia de la cuestión se hace más notoria si se contrasta con el hecho de que ninguno de nosotros nos desprendemos habitualmente de nuestros teléfonos celulares, y que en la actualidad se trata de accesorios que parecen formar parte de la anatomía de la mayoría de los individuos.

Sin perjuicio de que esta medida probatoria –al igual que la solicitud del registro de las direcciones de IP– no se encuentra específicamente regulada en nuestro ordenamiento procesal, resulta necesario priorizar una interpretación constitucionalizada de las normas procesales y

4 Al respecto, ver https://www.p-lib.es/derechos-y-libertades/sms-invisibles; y en el mismo sentido, https://www.genbeta.com/activismo-online/la-policia-usa-mensajes-de-texto-invisibles-para-localizar-y-rastrear-moviles

orgánicas que regulan las funciones propias de los agentes del Ministerio Público Fiscal (art. 93 CPPCABA y 20 de la Ley 1903), de modo tal que resulten compatibles con el esquema de división de funciones que prevé el sistema acusatorio previsto por el art. 13.3 CCABA, sobre el cual se estructura nuestro diseño procesal.

Frente a la aparición de nuevas formas de criminalidad que requieren de especiales técnicas de investigación y de nuevos medios de prueba, y frente a la irrupción de nuevas tecnologías de la información, es indispensable no sólo redimensionar el alcance de la garantía de la intimidad para extender el ámbito de protección desde el mundo físico hacia el entorno digital, sino también el alcance de la labor jurisdiccional.

El rol del juez de garantías en la etapa de investigación preparatoria no puede quedar reducido a la simple emisión de órdenes de allanamientos, requisas o interceptaciones de comunicaciones, ya que estas medidas de prueba fueron ideadas exclusivamente para investigación de hechos acontecidos en el mundo *físico* y no en el mundo *digital*.

De lo contrario, frente al auge de nuevas técnicas de investigación y las nuevas formas de vigilancia, quedaría absolutamente desbalanceado el esquema de distribución de competencias entre el órgano de acusación encargado de impulsar la investigación y el órgano jurisdiccional encargado de decidir y de velar por las garantías del imputado con carácter *previo* a la consumación de la injerencia estatal.

En este último esquema, las posibilidades reales de ejercer el rol jurisdiccional de velar por el respeto por las garantías frente a una serie de medidas que tienen la potencialidad de impactar en un altísimo grado sobre la vida privada de las personas, quedaría reducido a una mínima expresión.

En síntesis, antes del desarrollo de internet y del auge de la sociedad de la información y del conocimiento, las fronteras de la privacidad eran tangibles, y estaban definidas espacio-temporalmente, por ciertas barreras de carácter físico. Sin embargo, en la sociedad moderna esas barreras tradicionales se fueron tornando progresivamente más difusas, por lo que es necesario dimensionar la relevancia e impacto que tiene esta cuestión para poder redefinir el alcance con el que tradicionalmente se interpretaron ciertas

garantías, como así también el rol de cada uno de los operadores del proceso frente a los nuevos medios de prueba disponibles en la sociedad de la información y del conocimiento.

Con relación a esto último, la Corte IDH sentenció que *"(l)a fluidez informativa que existe hoy en día coloca al derecho a la vida privada de las personas en una situación de mayor riesgo debido a las nuevas herramientas tecnológicas y su utilización cada vez más frecuente. Este progreso, en especial cuando se trata de interceptaciones y grabaciones telefónicas, no significa que las personas deban quedar en una situación de vulnerabilidad frente al Estado o los particulares. De allí que el Estado debe asumir un compromiso, aún mayor, con el fin de adecuar a los tiempos actuales las fórmulas tradicionales de protección del derecho a la vida privada"* (Corte IDH, caso *"ESCHER y otro v. Brasil"*. Excepciones Preliminares, Fondo, Reparaciones y Costas, del 6 de junio de 2009. Serie C Nº 200; párr. 105).

La misma preocupación la expresaba en los albores del siglo XX el entonces magistrado de la Corte Suprema de Estados Unidos, Louis D. Brandeis, cuando se apartó la de la interpretación literal de la Cuarta Enmienda, al fundamentar su voto disidente en el conocido precedente *"OLMSTEAD v. United States"* (277 US 438, 465, 466, 1928), reivindicando una interpretación dinámica de la Constitución que permitiera adaptar las garantías constitucionales individuales establecidas frente a los abusos del poder a los cambios operados en los ámbitos político y social.

Ya para ese entonces manifestaba la preocupación que le generaban los avances tecnológicos invasivos de la privacidad, argumentando que frente al poder del gobierno los autores de la Constitución consagraron en favor del pueblo, como derecho más valioso, *"the right to be let alone"* (el "derecho de ser dejado a solas"), y que toda intrusión injustificada de las autoridades estatales en la esfera privada de la personas, cualesquiera que fuesen lo medios utilizados, constituye una violación de la garantía de la privacidad.

El propio Brandeis denunciaba la potencial invasión estatal de la esfera privada por avanzados dispositivos de reproducción o grabación, argumentando que el descubrimiento y la invención de mecanismos más sutiles y de mayor capacidad de invasión de la privacidad permitirían al

Gobierno asaltar la esfera personal individual, revelándose en los tribunales lo que es susurrado en la intimidad.

Sintetiza bien la cuestión el Observatorio Iberoamericano de protección de datos al describir -en el año 2014-: "*Hoy en día, en un mundo digitalizado, la naturaleza de la información es diferente a la que disponíamos en el pasado. Es así debido a la abundancia de orígenes disponibles, cada uno con su peculiar variedad de datos. Un tipo de fuentes son las que se refieren a datos creados directamente por las personas, como pueden ser la informática tradicional corporativa, redes sociales, transacciones de comercio electrónico, formularios web, blogs, centros de atención a clientes, etc. y sus posibles indexaciones en motores de búsqueda. Otro tipo, que se prevé sea dentro de poco el segmento más grande de toda la información disponible, se refiere a los datos obtenidos por máquinas, como pueden ser sensores, micrófonos, cámaras de video, escáneres médicos, equipos industriales, GPS, dispositivos móviles, nuevas generaciones de electrodomésticos, electrónica para vestir (wearable devices), etc. que también puede ser indexado. Todos estos tipos de datos forman parte del tejido de nuestras vidas más profundamente que nunca. La recolección, el almacenamiento, el procesamiento y el posterior análisis de datos se encuentra en una fase de expansión paradigmática, impulsada por el aumento de la capacidad de procesamiento y el creciente número de tecnologías integradas en dispositivos de todo tipo. (...) Cuando una compañía suministra los datos o la información de un usuario a un estado en respuesta a una solicitud que contravenga el derecho a la privacidad según el derecho internacional, o una empresa ofrezca tecnología de vigilancia de masas o equipos a los estados sin salvaguardas adecuadas, o cuando la información se utiliza de alguna manera en violación de los derechos humanos, las empresas corren el riesgo de ser cómplices o verse involucrados en violaciones de los derechos humanos."*[5]

En este contexto, tal como lo propuse al expedirme respecto de la viabilidad de la medida probatoria analizada en primer lugar, considero que

5 *"Hacia la implantación de garantías para la privacidad en los tratamientos de Big Data",* Declaración de México D. F. de 2014, disponible en http://oiprodat.com/wp-content/uploads/2014/08/Declaraci%C3%B3n-de-M%C3%A9xico-DF.pdf

resulta fundamental privilegiar una interpretación amplia y dinámica del derecho a la intimidad, principalmente teniendo en cuenta que la cláusula constitucional local prevé específicamente que se requiere orden judicial para acceder a la *"información personal almacenada"* (art. 13.8 CCABA), de conformidad con la interpretación progresiva que debe hacerse de dicha protección constitucional en virtud de lo dispuesto por el art. 33 CN, y de la interpretación que he propuesto previamente respecto del alcance del derecho a la autodeterminación informativa.

Frente a la solicitud de determinación de las celdas correspondientes a un teléfono móvil, los desarrollos tecnológicos modernos cuentan con aptitud suficiente como para revelar tanto el lugar en cuyas cercanías se encuentra un dispositivo de telefonía móvil en un momento determinado, como las ubicaciones en las que ha estado en momentos anteriores, o bien el recorrido que estimativamente podría atravesar en el futuro.

Si bien la medida dispuesta por el titular de la acción apunta a conocer los datos acontecidos en el pasado, lo cierto es que la tecnología actual permite un grado de especificidad tal que incluso resultaría posible requerir datos referidos a tiempo real, que obran en las bases almacenadas de la empresa prestataria del servicio.

En efecto, la generalizada utilización del teléfono móvil por parte de la mayoría de los miembros de las comunidades en la sociedad moderna, y la posibilidad de obtener una georreferenciación constante con independencia del conocimiento y de la voluntad de los usuarios, permite afirmar que la localización a través de la telefonía móvil constituye una de las herramientas más modernas para situar personas en el espacio en un momento determinado, desplazando otras clases de vigilancia.[6]

Es innegable la utilidad procesal que podría ostentar esta medida en el marco de las investigaciones criminales. Pero sería un gran error considerar

---

6 Así, por caso, en el sitio https://www.zeit.de/datenschutz/malte-spitz-data-retention puede visualizarse un ejemplo impactante de cómo la información aportada por las empresas de telefonía móvil permiten observar todos los movimientos de un diputado alemán del Partido Verde durante un período de tiempo prolongado. Ese monitoreo se realizó a partir del entrecruzamiento de datos de localización que poseen almacenadas las empresas prestatarias del servicio de telefonía móvil y otras fuentes de información disponibles públicamente

que esta última circunstancia, aisladamente considerada, alcanza para legitimar al titular de la investigación a requerir esa información autónomamente, cualquiera sea el estado procesal de la causa y el grado de sospecha que haya logrado reunir respecto de la hipótesis que persigue.

Antes bien, la intervención jurisdiccional constituye una garantía necesaria en virtud del innegable impacto que esta clase de medidas generan desde la perspectiva de la intimidad.

Con relación a esta temática, el TEDH ha interpretado que la práctica estatal de conservar datos de localización de un individuo constituye una injerencia en la vida privada de las personas aún cuando se trate de datos recogidos en lugares públicos (TEDH, *"AMANN c. Suiza"*, rta. 16/02/2000, párr. 65-67 y *"ROTARU c. Rumania"*, rta. 4/05/2000, párr. 43-44; más recientemente *"SHIMOVOLOS c. Rusia"*, rta. el 21/06/2011 en un caso referido al archivo de datos por parte del Estado de desplazamientos de un ciudadano a través de viajes en avión y tren).

Por otra parte, estas preocupaciones también fueron atendidas muy recientemente por la Corte Suprema de Estados Unidos, al resolver el caso *"CARPENTER v. United States"* (rta. el 22/06/2018), en el que se estableció por mayoría que para obtener las celdas de localización de un teléfono celular en una investigación criminal, se requiere una orden judicial de registro, que se adecue al estándar probatorio de la *"expectativa razonable de privacidad"*, ya que se trata de una medida que impacta en la garantía consagrada por la Cuarta Enmienda.

De hecho, la Corte de Estados Unidos concluyó que para que procediera la medida en se requería el mismo estándar de convicción que para la emisión de una orden de intervención telefónica o un allanamiento. Sostuvo así que no alcanzaba con los *"motivos suficientes"* dijo que se requería una orden judicial de registro fundada en *"causa probable"*[7].

---

7 Los investigadores habían accedido a los registros de las celdas en virtud de una orden judicial prevista por la *"Stored Communications Act"*, que requería que se demostrara que existían *"motivos fundados"* para creer que los registros eran relevantes para la investigación en curso (18 U. S. C. §2703(d). Esa demostración exige un estándar probatorio muy inferior que el de *"causa probable"* requerido para una orden de registro (*"United States v. Martínez-Fuerte"*, 428 U. S. 543, 560–561 (1976). Bajo el estándar previsto por la SCA, en cambio, sólo se debía acreditar que la prueba de las celdas de geoposicionamiento *podía ser relevante* para una investigación en curso.

El Juez Roberts, actual Presidente de dicho tribunal, lideró el voto de la mayoría, reconociendo justamente que el desarrollo de la tecnología requiere que se encuentren formas de preservar la privacidad de los ciudadanos de las injerencias del estado, frente a herramientas de investigación que permiten a las autoridades acceder a áreas que normalmente estaban fuera de la vista de los investigadores.

En particular, enfatizó que el hecho de que la información en cuestión obrara en poder de las empresas prestatarias del servicio como consecuencia de una entrega voluntaria de parte de los usuarios, no alcanzaba para interpretar una pérdida de interés en la privacidad de esa información.

Máxime si se tiene en cuenta que la información que almacenan las empresas no es información que el usuario les *"entrega"*, en el sentido estricto del término, ya que no existe ningún *acto afirmativo* del usuario que habilite a que las empresas de telecomunicaciones almacenen y suministren sus datos de *localización*, sino que los dispositivos de telefonía móvil van generando esos registros automáticamente para permitir el acto de comunicación -o incluso en total ausencia de un acto comunicacional-, siendo que es esta última, y no otra, la finalidad propia de dichos dispositivos.

A pesar de que la localización de los usuarios a través de las antenas de las empresas de telecomunicaciones puede constituir un elemento necesario para la operatividad del servicio, de todas maneras el *servicio* al que suscribe un usuario que utiliza un teléfono móvil es el de servicio de telecomunicaciones y no el de geolocalización.

En función de ello, creo que es posible sostener válidamente que la sociedad en su conjunto tiene una expectativa legítima de que las agencias estatales, a través de las entidades prestatarias del servicio de comunicaciones, no monitoreen sus movimientos.

Con relación a esto último, resulta especialmente interesante recordar que en sus anteriores precedentes vinculados a la interpretación del alcance de la garantía consagrada por la Cuarta Enmienda de la Constitución, la Corte estadounidense había establecido la denominada *"third party doctrine"* ("doctrina de terceros") según la cual los individuos no se encontraban protegidos por dicha cláusula constitucional respecto de los

registros que eran de titularidad o que eran controlados únicamente por un tercero.

Así, en el caso "*MILLER"* (425 U. S., at 437438) referido a la obtención de registros bancarios de un ciudadano sin orden judicial, y en *"SMITH"* (442 U. S., at 737) referido a los registros de las llamadas salientes de un teléfono fijo, obtenido también sin orden judicial, el tribunal había interpretado que las autoridades no habían registrado nada que efectivamente perteneciera a los sujetos investigados.

El fundamento de la aplicación de esta doctrina en este último caso fue que cuando un individuo realiza una llamada, voluntariamente habilita a que la compañía prestadora del servicio accediera a esos registros que hacen a la corriente diaria del servicio que la empresa presta.

Sin embargo, al revisar la naturaleza de la medida vinculada con la solicitud de registros de celdas de geoposicionamiento, tuvo especialmente en cuenta que el nivel de especificidad y detalle de la información que permite acceder esta prueba es muy parecida a la del GPS de un vehículo, y que no requiere ningún esfuerzo producirla.

El propio Juez Roberts reconoció en su voto que cuando se gestó la *"third party doctrine"* (1979) nadie podía imaginar una sociedad en la cual las personas vamos acompañadas de un dispositivo móvil con las características actuales, suministrando a las compañías involucradas en el sector, entre ellos los de telefonía celular, como en el caso, no sólo los registros de las llamadas que realiza, sino también un detallado registro de muchísimos de los movimientos de las personas.

En definitiva, lo interesante pasa por admitir que el hecho de que cierta información personal de un usuario se encuentre almacenada por las empresas de telecomunicaciones, por sí solo no permite sortear el derecho del usuario de reclamar la protección de su privacidad y la obligación positiva del estado en protegerla con los debidos contralores para acceder a ella.

Esta conclusión se ve reforzada, en el caso en concreto, por el hecho de que la geolocalización de un individuo ni siquiera forma parte del servicio específico que la empresa le presta a los ciudadanos.

Sólo quisiera agregar que el requisito referido a la exigencia de una orden judicial, como así también el estricto escrutinio al que se debe someter esta clase de medidas, en atención a su naturaleza y gravitación constitucional, no puede quedar relativizado por la gravedad o el carácter aberrante de los delitos que se persiguen, ni mucho menos por criterios de pragmatismo o de celeridad; máxime cuando no se verifican en el caso, ni tampoco han sido alegadas, razones de urgencia para proceder autónomamente.

En este sentido, siguen vigentes a pesar del tiempo transcurrido, las reflexiones del ex Ministro Petracchi de la CSJN al emitir su voto en el conocido precedente referido a la garantía de la inviolabilidad del domicilio, *"FIORENTINO"*, rta. 27/11/1984, con remisión a un párrafo del Juez Frankfurter en el precedente *"ESCOBEDO v. Illinois"* (378, US, 478, p. 490), cuando señalaba: *"Por medio de la declaración de Derechos, los fundadores de este país subordinaron la acción judicial a restricciones legales, no para conveniencia de los culpables sino para protección de los inocentes…"* y *"Podemos afirmar, con certeza, que el delito se combate con mayor eficacia cuando se cumplen rigurosamente los principios que han inspirado las restricciones constitucionales sobre la acción de los policías"*.

Siguiendo tales lineamientos, por la trascendencia actual y potencial de la medida desde la perspectiva de la intimidad, entiendo que la medida requerida puede proceder únicamente por orden judicial, luego de someterla a un escrutinio estricto, siempre que haya causa probable de la comisión de un delito y de la posible participación en el hecho de determinada persona, y en la medida que la prueba resulte necesaria y proporcional en atención a la gravedad del delito investigado.

En razón de que no se cumplió con el requisito de orden judicial, y que la medida fue dispuesta sin expresión de fundamentos y sin antes obtener el resultado de las restantes medidas ordenadas, entiendo que corresponde declarar la nulidad del oficio dirigido a la empresa de telefonía celular correspondiente, librado por el señor Fiscal en la presente causa.

Por las razones expuestas precedentemente, es que **RESUELVO:**

I. Librar oficio a la firma FACEBOOK INC., a fin de que informe los siguientes datos respecto del usuario con URL http://www.facebook.com/xxxxxx ID 00000000, asociado al abonado telefónico +5400000000 y al correo electrónico xxxxxxx@hotmail.com, **a.** Del Registro de Información Transaccional; **b.** Registro de direcciones IP utilizadas para el acceso, con indicación de las fechas y horas pertinentes; **c.** Información Registrada del usuario en cuestión; **d.** Abonado telefónico registrado por el usuario;

II. Librar oficio a la firma MICROSOFT INC. respecto del usuario identificado como titular de la cuenta de correo electrónico xxxxxxx@hotmail.com. **a.** Del Registro de Información Transaccional; **b.** Del Registro de direcciones IP utilizadas tanto para la creación como para el acceso hasta el presente, con indicación de las fechas y horas pertinentes; **c.** Información Registrada del usuario; **d.** Información sobre eventuales cambios de contraseña y las distintas y/o sucesivas cuentas de correo; **e.** Abonado telefónico registrado por el usuario;

III. DISPONER que, a fin de que la información sea recibida con mayor celeridad, el diligenciamiento de los mencionados oficios quede a cargo del Cuerpo de Investigaciones Judiciales como así también que no se informe al usuario de las cuentas que se está requiriendo judicialmente información del mismo bajo la leyenda *"se solicita no dar aviso al usuario de este requerimiento"*.

IV. HACER SABER a la Fiscalía interviniente que una vez concluida la investigación, tanto el señor Fiscal como el Cuerpo de Investigaciones Judiciales deberán proceder a la destrucción de todos los datos y registros que no guardan trascendencia para la investigación, que obren en su poder (art. 4 inc. 7º de la Ley 25.326).

V. DECLARAR LA NULIDAD de las medidas dispuestas por el señor Fiscal relativas al pedido de informes cursados a la empresas de telefonía celular correspondiente al abonado +5400000000 en lo referido a la solicitud del listado de celdas de conexión habilitadas con su correspondiente ubicación geográfica.

VI. HACER SABER al señor Fiscal que deberá remitir a este tribunal los elementos probatorios cuya nulidad se ha declarado, a efectos de proceder a su destrucción.

VII. Regístrese, y de conformidad con lo aquí ordenado, remítase la presente causa a la Fiscalía interviniente, junto con los oficios ordenados.

En de agosto de 2018 se remitió el presente legajo a la Fiscalía PCyF Nro. 30, junto con dos (2) oficios.