**RESOLUCION INTERLOCUTORIA**

***Hace lugar al libramiento de oficios solicitando informes a la firma Google Inc.***

Buenos Aires, de octubre 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 Google para que informe los siguientes datos respecto del usuario de la dirección de correo electrónico [juandiaz00@gmail.com](mailto:luistaboada62@gmail.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; d. Abonado telefónico registrado por el usuario.

**ARGUMENTOS:**

**I.** Entiendo que cierta parte de la información de carácter personal que se requiere a la firma Google Inc. 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), 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.

Para mayor claridad, es posible tomar como punto de partida la *“Guía de buenas prácticas para obtener evidencia electrónica en el extranjero”,* elaborada por la Unidad Fiscal Especializada en Ciberdelincuencia Dirección General de Cooperación Regional e Internacional, de la Procuración General de la Nación, en el 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).

De acuerdo con ese documento, pueden establecerse tres grupos de información: básica, transaccional y de contenido.

La categoría de "información básica", incluye datos del titular de la cuenta, como puede ser nombre, país, dirección, teléfonos, edad, etc.; dirección de correo electrónico asociada (usada generalmente para verificar/recuperar la cuenta); número de teléfono celular asociado; número de tarjeta de crédito asociada; dirección IP desde la que se creó la cuenta; detalle de los últimos accesos a la cuenta (fecha, hora, zona horaria y dirección IP); e información sobre servicios a los que se ha suscripto el titular de la cuenta.

La categoría "información transaccional", se refiere a 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. En estos casos, el estándar es un poco más exigente que en el supuesto anterior.

Por último, la "información de contenido" consiste en el contenido (texto y adjuntos) de los correos electrónicos que permanezcan en las carpetas de la cuenta (enviados, recibidos, borrador, papelera, etcétera); contenido (texto y adjuntos) de los mensajes intercambiados en plataformas de redes sociales; contenido de publicaciones realizadas en redes sociales cuyo acceso fue restringido al público en general; y por último, el historial de localización asociado a una cuenta.

Si bien esta categorización, elaborada en función del menor o mayor grado de sensibilidad de la información que se pretende obtener, puede resultar de ayuda para fijar un parámetro sobre cuáles serían los informes que –de acuerdo con mi interpretación– los investigadores podrían requerir sin orden judicial, considero que resulta necesario realizar algunas precisiones para fijar parámetros de actuación claros.

Ante todo, entiendo que no resulta admisible admitir que los fiscales soliciten información denominada como “transaccional” y “de contenido”, en virtud del grado de sensibilidad de la información en cuestión.

Ahora bien, dentro de la primera categoría de la “información básica”, los datos vinculados al detalle de los últimos accesos a la cuenta con indicación de fecha, hora, zona horaria y dirección IP no puede recibir el mismo tratamiento que el resto de la información que una persona introduce de forma consciente al registrarse como usuario, como ser el nombre, el país, la dirección, teléfonos, edad, etc.; dirección de correo electrónico asociada; número de teléfono celular asociado; número de tarjeta de crédito asociada.

En cuanto al dato relativo a la dirección IP desde la que se creó la cuenta, si bien no se trata de una información que el usuario haya introducido de forma voluntaria, resulta razonable que pueda ser relevado sin orden judicial en la medida que se trata de un dato que, considerado de forma aislada, representa un grado de injerencia insignificante en la privacidad.

Lo mismo puede predicarse respecto del dato de la dirección de IP desde la que se habría generado el incidente presuntamente configurativo de un delito, al cual también entiendo que los investigadores pueden acceder autónomamente.

En efecto, así es como generalmente se inician este tipo de causas, a partir de la generación de un reporte derivado a las autoridades locales por parte de las plataformas digitales a través de NCMEC, en el que se consigna justamente una dirección de IP de creación de la cuenta y, en algunos casos, también la dirección de IP correspondiente al incidente denunciado.

Esto resulta legítimo si se tiene en cuenta que las plataformas digitales que dan origen a esos reportes establecen una serie de condiciones de uso que deben ser consentidas por los usuarios, y que contemplan específicamente la posibilidad de que se denuncie ante las autoridades que correspondan los eventos que posiblemente impliquen la comisión de un delito.

A tal fin, resulta indispensable para los investigadores conocer el presunto lugar de comisión del hecho, a lo que únicamente se puede acceder a través de la dirección de IP del evento denunciado y/o de la creación de la cuenta presuntamente utilizada con fines delictivos.

Sin embargo, como lo anticipé previamente, no puede perderse de vista que el acceso a la totalidad de los registros históricos de direcciones de IP de una cuenta del sujeto investigado representa un grado de injerencia en la intimidad del individuo muchísimo más importante, y que no se trata de información referida al evento que se reporta, que se encuentra temporalmente distanciada del incidente denunciado, por lo que mal podría interpretarse que su relevamiento también se encuentra abarcado a partir de la aceptación del usuario de ciertas condiciones de uso.

Repárese que ni siquiera las propias empresas que efectúan las denuncias vuelcan todos esos datos en los informes que remiten a NCMEC.

En este punto, es importante detenerse a evaluar que el listado de la totalidad de las direcciones de IP históricamente utilizadas por un usuario terminan aportando a los investigadores un listado de direcciones físicas desde las cuales se establecieron las distintas conexiones o accesos a una cuenta.

Sin lugar a dudas, ese conglomerado de información representa una invasión de mayor entidad en el ámbito de la privacidad del usuario investigado, ya que se refiere a períodos de tiempo que pueden llegar a ser muy prolongados, y que guardan una distancia ostensible respecto de la fecha de presunta comisión del delito investigado.

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*.[[1]](#footnote-1)

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 tecnológicos han permitido producir *“una imagen total y pormenorizada de la persona”* convirtiéndose así el ciudadano en *“hombre de cristal”*.[[2]](#footnote-2)

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”.*

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.

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 la Fiscalía, 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), en los reportes Nº 12121212 y 34343434 de los que surge que los usuarios de la red Skype juandiaz00 y familiadiaz1 habrían facilitado imágenes en las que se observa a una niña menor de edad desarrollando actividades sexuales explícitas, y tiene por objeto recabar pruebas que permitan individualizar fehacientemente al usuario de dichas cuentas.

Previo a este pedido, la Fiscalía solicitó en forma autónoma la firma Skype que informara los datos de registración y conexión de ambos usuarios. Dicha firma respondió sólo por el primer usuario referido. Indicó la fecha de creación de la cuenta, la dirección de IP utilizada para ello, y aportó el mail de registración: [juandiaz00@gmail.com](mailto:luistaboada62@gmail.com) (pág. 16).

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.

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, autorizaré el libramiento de un oficio a Google, en los términos pretendidos por la Fiscalía.

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

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

**I. Librar oficio a la firma GOOGLE INC.**, a fin de que informe los siguientes datos del usuario de la dirección de correo electrónico [juandiaz00@gmail.com](mailto:luistaboada62@gmail.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; **d.** Abonado telefónico registrado por el usuario;

**II. 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”.*

**III. HACER SABER** a la Fiscalía interviniente que una vez concluida la investigación, tanto el 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).

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

El       de octubre de 2018 se remitió el presente legajo a la Fiscalía PCyF Nro. 7, junto con un (1) oficio.

1. 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-publishing.com/catalog/details//store/es/book/978-3-639-53666-9/di%C3%A1logo-de-fuentes-en-el-derecho-del-consumidor?locale=gb [↑](#footnote-ref-1)
2. 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/*](http://www.derecho-chile.cl/sentencia-de-15-de-diciembre-de-1983-del-tribunal-constitucional-federal-aleman-ley-del-censo/) [↑](#footnote-ref-2)