La recopilación de datos personales por las tecnológicas y los reclamos por eventuales daños a los usuarios: La sentencia dictada por la Corte Suprema de Reino Unido, en el caso Lloyd vs Google LLC [2021]

Marianela Zubillaga*

RVDM, Nro. 11, 2023, pp. 325-346

Resumen: Los datos personales tienen un valor económico, particularmente cuando se recogen a gran escala, lo que ha generado la llamada "economía del dato". El recono- cimiento del derecho a la protección de datos personales como un derecho inherente al ser humano, ha hecho que los países dicten normas de protectoras en esta materia. En este contexto, han surgido reclamos contra las grandes tecnológicas, por haber recabado datos sin autorización de los usuarios, lo cual ha generado discusiones en los foros judiciales de otras latitudes, sobre la procedencia o no de tales reclamos, de los daños ocasionados y de ser el caso y del derecho a obtener o no una indemnización.

Palabras claves: Datos personales, economía del dato, empresas tecnológicas.

The collection of personal data by technology companies and claims for possible damages to users: The ruling handed down by the Supreme Court of the United Kingdom, in the case Lloyd vs Google LLC [2021]

Abstract: *Personal data have an economic value, particularly when collected on a large scale, which has led to the so-called "data economy." The recognition of the right to the protection of personal data as an inherent human right has led countries to enact protective regulations in this area. In this context, claims have arisen against the big tech companies for having collected data without the authorization of users, which has generated discussions in the judicial forums of other latitudes, about the admissibility or not of such claims, the damages caused and, if appropriate, the right to obtain or not an indemnity.*

Keywords: *Personal data, data economy, tech companies.*

Recibido: 20/11/2023
Aprobado: 28/11/2023

* Abogado *Cum-laude* Universidad Católica Andrés Bello (1988). Profesora Asistente Derecho Mercantil (Prácticas) y Fundamentos Derecho Mercantil (2011-2021). Abogado socia de Baumeister & Brewer, abogados consultores.

La recopilación de datos personales por las tecnológicas y los reclamos por eventuales daños a los usuarios: La sentencia dictada por la Corte Suprema de Reino Unido, en el caso Lloyd vs Google LLC [2021]

Marianela Zubillaga*

RVDM, Nro. 11, 2023, pp. 325-346

SUMARIO:

INTRODUCCIÓN

Nos encontramos inmersos en un acelerado avance y cambio de la sociedad, ante la irrupción del fenómeno digital y tecnológico en todas las esferas de la vida, tanto en lo privado como en lo público. No hay escapatoria a la realidad digital y a los avances de la tecnología.

Frente a ello, se destaca que el núcleo de este avance es el dato. Así lo afirma la comunicación de la Comisión de la Unión Europea (UE) al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, al señalar que:

> "Los datos están en el centro de esta transformación, y va a ir a más. La innovación basada en los datos reportará enormes beneficios a los ciudadanos, por ejemplo, mediante la mejora de la medicina personalizada, la nueva movilidad y su contribución al Pacto Verde Europeo. En una sociedad en la que las personas generarán cantidades cada vez mayores de datos, la manera en que se recogen y utilicen los datos debe situar los intereses de la persona en primer lugar, de conformidad con los valores, los derechos fundamentales y las normas europeos. Los ciudadanos solo confiarán y harán suyas las innovaciones basadas en los datos si confían en que todo intercambio de datos personales en la UE estará sujeto al pleno respeto de sus estrictas normas en materia de protección de datos. Al mismo tiempo, el volumen cada vez mayor de datos industriales no personales y de datos

* Abogado *Cum-laude* Universidad Católica Andrés Bello (1988). Profesora Asistente Derecho Mercantil (Prácticas) y Fundamentos Derecho Mercantil (2011-2021). Abogado socia de Baumeister & Brewer, abogados consultores.

> públicos en Europa, junto con el cambio tecnológico en el modo de almacenamiento y tratamiento de los datos, constituirá una fuente potencial de crecimiento e innovación que debe aprovecharse"[1].

Observamos entonces, que los datos personales tienen un valor económico, fundamentado, no tanto en cada dato individualmente considerado, sino –y muy especialmente– en lo que se puede obtener de dichos datos cuando se recopilan, almacenan y tratan en gran cantidad, así como cuando se unen con otros. De manera que, es esa posibilidad de su recopilación, tratamiento y vinculación con otros datos y la información que de allí se extraiga lo que ha generado la llamada "economía del dato"[2] a través del *big data*[3]. El uso y la aplicación de tal información a la creación de patrones de consumo, perfilamiento de gustos y otros usos, conduce a la obtención de lucro por parte de quienes recopilen, manejen y compartan tales datos, creando así un modelo de negocios soportado en la información que de allí se obtiene.

En este contexto, las grandes empresas tecnológicas detectaron que la recolección de datos de forma masiva, así como ciertos atributos que tienen las redes sociales[4]

---

1 "Una estrategia europea para los datos" (Bruselas, 19 de febrero de 2020) Pág., 4. Consultado en https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

2 "La economía de los datos mide la repercusión global del mercado de los datos –es decir, el mercado en que se intercambian datos digitales como productos o servicios derivados de los datos brutos– en el conjunto de la economía. Implica la generación, recogida, almacenamiento, procesamiento, distribución, análisis, elaboración, entrega y explotación de los datos que hacen posibles las tecnologías digitales (*European Data Market study*, SMART 2013/0063, IDC, 2016)". Tomado de la "Comunicación De La Comisión Al Parlamento Europeo, Al Consejo, Al Comité Económico Y Social Europeo Y Al Comité De Las Regiones «La Construcción De Una Economía De Los Datos Europea» Bruselas, 10 de enero de 2017. consultado en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52017DC0009&from=EN#footnote2

3 Se entiende por *Big Data* a "… la gestión y análisis de enormes volúmenes de datos que no pueden ser tratados de manera convencional, ya que superan los límites y capacidades de las herramientas de software habitualmente utilizadas para la captura, gestión y procesamiento de datos. Dicho concepto engloba infraestructuras tecnológicas y servicios que han sido creados para dar solución al procesamiento de enormes conjuntos de datos estructurados, no estructurados o semi-estructurados (mensajes en redes sociales, señales de móvil, archivos de audio sensores, imágenes digitales, datos de formularios, emails, datos de encuestas, logs, etc…" Tomado de https://www.eleconomista.es/diccionario-de-economia/big-data

4 Los botones "me gusta" de Facebook o el de "retuitear" de Twitter permiten conocer gustos, preferencias e inclinaciones de las personas. Así lo indica BLANCO, Luis Ernesto, en su artículo "Dame tus «likes» para mentirte mejor", en el cual señala que: "Entre finales de 2008 e inicios de 2009 Facebook realizó un pequeño ajuste a su interfaz, que cambió de forma definitiva la manera de interactuar con el contenido que se ve dentro y fuera de esta red social: el botón Like («me gusta») que está por todos lados y le permite mostrarle al mundo sus preferencias al navegar por internet. Cada «me gusta» que deja en las redes sociales construye una base de datos acerca de su personalidad, gustos y creencias: el sueño de cualquier dirección de mercadeo". "Debates IESA", 16 octubre, 2018, consultado en: http://www.debatesiesa.com/dame-tus-likes-para-mentirte-mejor/
Por otra parte, debemos recordar que el desarrollador del botón *retuit* en Twitter, Chris Wetherell, en una entrevista para Buzzfeed, dijo que no había sido una buena idea, porque fue como
"… entregar un arma cargada a un niño de c,uatro años. Según Wetherell esta función ha favorecido que se compartan los contenidos de forma excesiva, y fuera de control, ya que los usuarios lo hacen sin haber contrastado el contenido que comparten.
(…)
Además, el *retuit* se puede usar para coordinar ataques contra determinados objetivos diseminando información falsa a un ritmo que hace difícil la respuesta por parte del objetivo de la campaña de difamación, (…)

les permiten conocer los gustos y opiniones de las personas de primera mano, una información inestimable y con un valor mucho mayor que aquella que se obtiene a partir de encuestas o estudios de mercado y a un menor costo. Toda esta información tiene valor económico, ya que permite ofrecer a los anunciantes, que envíen publicidad personalizada a cada internauta y así ha sido utilizada por las grandes empresas tecnológicas[5].

Una de esas empresas que recabó datos sin la autorización de los usuarios, fue Google, quien, a través del buscador Safari, obtuvo datos personales de los usuarios de dicho navegador sin su consentimiento o autorización, tal como se desarrollará de seguidas.

1. El caso Lloyd vs Google LLC [2021][6]

Un exmiembro de una asociación de consumidores británica muy influyente, llamada, ¿Which? (¿Cuál?), el Sr., Richard Lloyd, respaldado por un financiador de litigios[7], constituyó la asociación "*Google You Owe Us*" ("Google, nos lo debes"), a los fines de incoar, en el año 2017, una acción colectiva (*class action*) contra Google LLC, en representación de más de cuatro millones de personas, usuarias de *iPhones*, entre 2011 y 2012, con fundamento en los hechos que se describen *infra*.

El caso se presentó, teniendo tres precedentes que fueron solventados en contra de Google: En primer lugar, en los Estados Unidos, Google aceptó pagar una multa

---

Por otro lado, la posibilidad que otorga el *retuit* de convertirse en viral y en una personalidad dentro de la red social, hace que la gente busque precisamente ser masivamente retuiteado y por tanto escriba mensajes injuriosos hacia alguien sólo para buscar que los detractores de aquel a quien va dirigido, los compartan sin tan solo leerlos.
En opinión de Wetherell, ha llegado el momento de arreglar esta situación, pero es complicado porque parte del ingreso publicitario de las redes sociales depende en gran medida de la capacidad que sus usuarios tengan de compartir los contenidos. Las marcas quieran la mayor difusión posible de sus contenidos y las redes sociales cobran en función de la exposición que estos contenidos tienen".
La Vanguardia, 25/07/2019, "El creador del botón de *retuit* se arrepiente de su idea" consultado en https://www.lavanguardia.com/tecnologia/actualidad/20190725/463690303652/ingeniero-responsable-boton-retweet-arrepiente.html#:~:text=Chris%20Wetherell%20fue%20el%20desarrollador,un%20ni%C3%B1o%20de%20cuatro%20a%C3%B1os

[5] La relevancia que tienen los datos y su recogida para cada persona y sus derechos se muestra de manera palmaria en un artículo de los abogados irlandeses Mark D. Finan BL y R. Caroline McGrath BL, que en un artículo sobre el tema destacan lo siguiente:
"Cada lector de este artículo es un titular de datos. Si lee el artículo en línea, ha creado datos que lo identifican directamente o que pueden hacerlo. Si lee muchos artículos jurídicos, los algoritmos pueden identificar una cierta preferencia y dirigir su atención hacia los artículos jurídicos. Esta es una empresa que utiliza datos sobre usted y busca utilizar sus preferencias para adoptar un marketing más eficiente (aunque se trate de un artículo jurídico). Cómo se recopilan, procesan y controlan esos datos es motivo de preocupación. Principalmente porque le conciernen a usted. Si sus datos se recogen con fines comerciales, debe ser informado de ello. Su consentimiento debe ser de suma importancia cuando se utilizan datos que son capaces de identificarlo". (Traducción libre).
Consultado en: https://www.lawlibrary.ie/viewpoints/gdpr-article-82/

[6] La sentencia se puede consultar en el siguiente enlace: https://www.bailii.org/uk/cases/UKSC/2021/50.html

[7] El financiador de litigios comerciales fue el *Therium Litigation Funding IC*, según el numeral 1 de la propia sentencia.

impuesta por la *Federal Trade Comission,* FDA (Comisión Federal de Comercio)[8] por la suma de 22,5 millones de dólares, en virtud de la denuncia ventilada en dicha comisión por la vulneración de la privacidad de los usuarios de Safari[9], a través de los dispositivos de *Apple*, al habilitar unas "*cookies*" de seguimiento (o *cookies* espías), que terminaron en dichos equipos, luego de que los usuarios visitaran sitios web en la red de publicidad de Google, *DoubleClick*, todo ello, sin el consentimiento, ni el conocimiento de los usuarios y a pesar de las garantías de que esta opción no estaba disponible, en virtud de la configuración por defecto del buscador Safari[10].

En segundo lugar –también en los Estados Unidos– en noviembre de 2013, Google convino pagar diecisiete millones de dólares, para resolver las demandas estatales de los consumidores, presentadas en su contra por treinta y siete fiscales generales de los estados de la Unión y el Distrito de Columbia, por los mismos motivos del caso en análisis[11].

---

[8] Para mayor información sobre este caso, ver: *Federal Trade Comission*, "Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser", consultada en: https://www.ftc.gov/news-events/news/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented-privacy-assurances-users-apples

[9] Safari es un navegador de Internet desarrollado por *Apple* e instalado en sus *iPhones*.

[10] Según lo indicado por la FDA, Google insertó un código que eludía la configuración de privacidad del navegador de Apple, el cual sí bloqueaba por defecto las cookies de terceros. De esta manera, las cookies de seguimiento o "espías" le permitían al buscador recopilar información sobre la actividad en línea de los usuarios, como las páginas web que visitaban, los anuncios que veían o los términos de búsqueda que usaban, y utilizarla para ofrecerles anuncios personalizados en función de sus intereses, a través de su red de publicidad *DoubleClick.* Tal acción se realizó a pesar de que Google había asegurado previamente, a los usuarios de Safari, que no necesitaban hacer nada para evitar que la instalación de las cookies de seguimiento, porque el navegador las bloqueaba automáticamente.
Señaló la FDA que la citada conducta fue desplegada por Google en violación a un acuerdo previo que había firmado con dicha entidad en el año 2011, a través del cual se había comprometido a ser transparente con los usuarios sobre sus prácticas de privacidad y a requerir su consentimiento expreso, antes de recopilar o compartir sus datos personales. Ver: https://www.ftc.gov/news-events/news/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented-privacy-assurances-users-apples

[11] El Departamento del Protección al Consumidor del Estado de Connecticut emitió un comunicado el 18 de noviembre de 2013, en el cual afirmó lo siguiente sobre dicho caso:
"Los estados alegaron que desde el 1 de junio de 2011 hasta el 15 de febrero de 2012, Google eludió la configuración de privacidad predeterminada de Safari, sin el conocimiento y consentimiento de los consumidores, permitiendo a los anunciantes establecer cookies de terceros en los navegadores de los usuarios. Según los estados, estas leyes contradecían las garantías de Google a los consumidores de que la configuración de privacidad predeterminada de Safari bloquearía dichas cookies de terceros.
Google afirmó que los consumidores podrían evitar que se colocaran cookies de terceros en sus navegadores web Safari simplemente confiando en la configuración predeterminada del navegador, dijo el Fiscal General Jepsen. (…) Google en realidad estaba eludiendo esas mismas configuraciones de privacidad y colocando cookies de anunciantes en los navegadores Safari de los consumidores, sin su conocimiento o consentimiento.
Los consumidores merecen saber cuándo otros utilizan su actividad en Internet y deberían poder tomar medidas para evitarlo", afirmó el Comisario Rubenstein. "No toleraremos el engaño que socava la capacidad de los consumidores de elegir por sí mismos la información que les gustaría compartir.
(…)
El acuerdo prohíbe a Google emplear cualquier funcionalidad HTTP Form POST que utilice javascript para anular la configuración de bloqueo de cookies de un navegador sin el consentimiento del consumidor, a menos que sea para evitar fraudes o abordar otros problemas técnicos o de seguridad. Google deberá proporcionar información consolidada sobre las cookies y su uso durante los próximos cinco años.
El acuerdo también prohíbe a Google tergiversar u omitir datos materiales sobre cómo los consumidores pueden usar la

En tercer lugar, en el Reino Unido, tres ciudadanos también demandaron a Google, en junio de 2013, con fundamento en la misma acusación[12], reclamando una compensación por uso indebido de información privada. El caso llegó hasta la Corte Suprema, pero antes de que dictara una decisión, –en marzo de 2015– Google firmó con los demandantes, un acuerdo de carácter confidencial.

1.1. Los hechos

En el caso en estudio, el demandante Lloyd alegó que Google había violado las normas de privacidad del navegador Safari y la normativa de protección de datos vigente para ese momento, al rastrear –en secreto– la navegación en línea de los usuarios.

Concretamente, conforme a lo que consta en la sentencia, el demandante sostuvo que Safari –a diferencia de la mayoría de los otros navegadores de Internet– estaba configurado de manera predeterminada para bloquear las *cookies* de terceros[13]. Por su parte, Google tenía una *cookie* conocida como "cookie de anuncios de *DoubleClick* " que podía funcionar como una cookie de terceros, la cual se instalaba en un dispositivo, si el usuario visitaba un sitio web que incluyera dicha cookie. Al instalarse en cada dispositivo, la cookie de anuncios de *DoubleClick* permitía a Google identificar las visitas del dispositivo a cualquier sitio web que tuviera un anuncio de su amplia red publicitaria y recopilar una gran cantidad de información, ya que podía identificar la fecha y la hora de cualquier visita, el tiempo que el usuario pasaba en él, los anuncios que fueron vistos y durante cuánto tiempo; incluso, en algunos casos, mediante la dirección IP del navegador, se podía identificar la ubicación geográfica aproximada del usuario.

---

herramienta de configuración de anuncios de Google o cualquier otro producto, servicio o herramienta de Google para administrar directamente cómo Google muestra anuncios en sus navegadores. Además, Google debe mantener sistemas configurados para indicar a los navegadores web Safari que caduquen las cookies infractoras".
Consultado en: https://portal.ct.gov/DCP/News-Releases-from-the-Department-of-Consumer-Protection/2013-News-Releases/Connecticut-36-Other-States-Reach-17M-Settlement-with-Google (Traducción libre)

[12] Es el denominado Caso Vidal Hall V Google Inc.
En la sentencia de instancia, se identifica como "*cookie intermediaria*" y se indica que:
"La cookie intermediaria fue diseñada por la demandada de tal forma que se envió a los navegadores Safari con la configuración de privacidad predeterminada… Como resultado, la cookie intermediaria se envió automáticamente a los navegadores de usuarios de Safari que no habían cambiado su configuración de privacidad predeterminada y que accedieron a los servicios de internet del demandado durante el período relevante. Además, fue enviado sin el conocimiento o consentimiento de dichos usuarios. Al igual que la cookie de *DoubleClick*, la cookie intermediaria fue, en todos los momentos relevantes, una cookie de terceros asociada al dominio doubleclick.net". Traducción libre.
Con relación al reclamo, los tres demandantes alegaron que el uso indebido de información y/o abuso de confianza, por parte de Google, afectó y dañó su dignidad personal, la autonomía y la integridad, y reclamaron daños y perjuicios por ansiedad y angustia, no reclamando en ningún momento pérdida económica u otro daño material. La sentencia de instancia se puede consultar en: https://www.ucpi.org.uk/wp-content/uploads/2018/03/Vidal-Hall-v-Google-Inc-Information-Commissioner-intervening-2015-EWCA-Civ-311-2016-QB-1003.pdf

[13] Una "*cookie de terceros*" es aquella instalada en el dispositivo, no por el sitio web visitado, sino por un tercero, cuyo contenido está incluido en dicho sitio. Las *cookies de terceros* son utilizadas para la recopilación de información sobre el uso de Internet y, en particular, sobre las páginas web visitadas, así como enviar al usuario anuncios adaptados a los intereses, deducidos de su historial de navegación.

Adicionalmente, el demandante señaló que también se recogieron otros datos como sus intereses y pasatiempos, raza o etnia, clase social, política o creencias o afiliaciones religiosas, salud, intereses sexuales, edad, sexo y situación económica[14].

Aunque la configuración predeterminada de Safari bloqueaba todas las cookies de terceros, una aplicación general de esta configuración impedía el uso de ciertas funciones web populares, por lo que Apple ideó algunas excepciones para ellos, las cuales estuvieron vigentes hasta marzo de 2012, cuando se cambió el sistema. No obstante, mientras estuvieron vigentes dichas excepciones, fue posible que Google colocara la cookie de anuncios de *DoubleClick* en un dispositivo Apple, cada vez que el usuario visitaba un sitio web que contenía anuncios de este tipo, sin el conocimiento o consentimiento del usuario.

Además, el demandante agregó que Google generó información de los usuarios que mostraban patrones similares, creando grupos con etiquetas como "amantes del fútbol" o "entusiastas de la actualidad". Con esta información, el servicio *DoubleClick* de Google ofrecía estos grupos "etiquetados" a los anunciantes suscritos, para que eligieran las categorías de personas a quienes querían enviar sus anuncios[15].

Según lo señalado por el demandante, con esta conducta, –al igual que en Vidal Hall– Google incumplió sus deberes como controlador de datos, conforme a la normativa de protección de datos vigente para ese momento[16], al rastrear en secreto la actividad en Internet de los usuarios de *iPhone* de *Apple*, recopilar y usar esos datos, y luego venderlos, es decir, con un uso comercial.

Lo novedoso de esta acción, –según la propia sentencia de la Corte Suprema– es que el Sr. Lloyd, no solo reclamó daños y perjuicios en nombre propio[17], sino que él sostuvo que la demanda había sido presentada en representación de todos los residentes en Inglaterra y Gales que poseían un *iPhone* de *Apple* en la época en que sucedieron los hechos (estimados en más de cuatro millones[18]) y cuyos datos Google obtuvo sin su consentimiento, por lo que, a su entender, él tenía derecho a reclamar daños y perjuicios en nombre de todas estas personas, a través de un recurso, en inglés denominado *class actions*[19] o acciones colectivas y solicitó una compensación de 750 libras esterlinas por persona.

---

[14] Ver párrafos 11 y 13 de la sentencia.

[15] Ver literal B de la sentencia.

[16] La norma vigente en el Reino Unido era la Ley de Protección de Datos de 1998 (DPA), tal como se desarrollará *infra*, que luego fue reemplazada por el Reglamento General de Protección de Datos de la UE, que se incorporó a la ley del Reino Unido después del Brexit.

[17] Como sí fue en el caso de Vidal Hall.

[18] Ver numeral 2 de la sentencia. Traducción libre

[19] Según el numeral 3 de la sentencia, este tipo de acciones no son comunes ni están reguladas en el derecho anglosajón, a diferencia de los Estados Unidos. Señala la sentencia que: "Las demandas colectivas, en las que se permite a una sola

Google por su parte, se opuso a los alegatos de Lloyd, sosteniendo que: (i) los demandantes de la acción no habían sufrido "daño" en el sentido de la sección 13 de la DPA; y (ii) se opuso a la acción colectiva, ya que, en su criterio, el Sr. Lloyd no tenía derecho a presentar un reclamo de esta naturaleza, dado que no todos tenían el mismo interés y no eran identificables.

El Tribunal de primera instancia falló a favor de Google, fundamentado en que, al no haber daños y perjuicios probados, no era procedente la acción, a tenor de la norma contenida en la sección 13 del texto legislativo, contra lo cual Lloyd apeló, argumentando que tal evaluación no era necesaria porque, al haber una pérdida de control de sus datos personales, todos deberían tener derecho a una "suma uniforme", por el monto estimado por él. El Tribunal de Apelación falló a su favor, y frente a tal decisión, Google apeló a la Corte Suprema.

1.2. El derecho aplicable

Para el momento de la ocurrencia de los hechos, la normativa vigente en el Reino Unido era la Ley de Protección de Datos de 1998[20]. Los artículos que entraron en discusión, –por lo que respecta al derecho subjetivo y no a las adjetivas, relativas a la procedencia o no de la *class action*, lo cual escapa del ámbito de este trabajo, pero se hará una breve referencia *infra*– fueron, fundamentalmente dos:

> La primera, la sección 4 (4), referida a los principios que deben orientar la recogida y tratamiento de datos personales, en donde se consagra la obligación del responsable del tratamiento (es decir la empresa que recoge y controla los datos), de cumplir con los principios que recoge la ley[21], los cuales se fundamentan en ocho[22], a saber:

persona presentar una demanda y obtener reparación en nombre de una clase de personas que se han visto afectadas de manera similar por supuestas irregularidades, han sido posibles durante mucho tiempo en los Estados Unidos y, más recientemente, en Canadá y Australia. Se ha discutido mucho si la legislación para establecer un régimen de acciones colectivas debería promulgarse en el Reino Unido. En 2009, el Gobierno rechazó una recomendación del Consejo de Justicia Civil de introducir un régimen genérico de demanda colectiva aplicable a todos los tipos de reclamos, prefiriendo un "enfoque basado en el sector". Traducción libre.

[20] *Data Protection Act 1998*, que entró en vigor en el Reino Unido el 16 de julio de 1998 y estuvo vigente hasta el 25 de mayo de 2018. Consultada en: https://www.legislation.gov.uk/ukpga/1998/29/contents/enacted
Esta ley inglesa fue dictada en ejecución de la "Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos", Diario Oficial L 281, 23/11/1995 P. 0031–0050. Consultada en: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046

[21] El artículo citado señala que: "Será deber del responsable del tratamiento cumplir con los principios de protección de datos en relación con todos los datos personales respecto de los cuales sea responsable del tratamiento". Consultada en: https://www.legislation.gov.uk/ukpga/1998/29/contents/enacted

[22] Ver Capítulo 1, de la Ley "Los principios de la protección de datos" Consultado en: https://www.legislation.gov.uk/ukpga/1998/29/schedule/1/enacted

i. Procesamiento justo y legal: Vela porque los datos sean recogidos y utilizados de forma justa y dentro de la ley. Este principio abarca la obligación, para quien recoge los datos de, en primer lugar, identificarse como el responsable del tratamiento, en segundo lugar, expresar la finalidad de su recogida y en tercer lugar, señalar si dichos datos serán compartidos y caso afirmativo con quienes se hará y en cuarto lugar, solicitar autorización[23].

ii. Limitación de la finalidad: Los datos deben ser procesados solo para los fines especificados al usuario.

iii. Adecuación y relevancia: Los datos recogidos deben ser adecuados, relevantes y no excesivos en relación con los fines para los que se procesan.

iv. Exactitud: Los datos deben ser precisos y mantenerse actualizados.

v. Limitación del almacenamiento: Los datos no deben ser conservados más tiempo del necesario, para los fines para los que son procesados.

vi. Procesamiento de acuerdo con los derechos del individuo: El procesamiento de los datos debe respetar los derechos del individuo.

vii. Seguridad: Los datos deben ser conservados de forma segura. Dentro de este principio se incluye la obligación de los procesadores de datos de tomar medidas para evitar el tratamiento no autorizado o ilícito de datos personales así como la destrucción, daño o pérdida accidental de datos personales.

viii. Transferencias internacionales: Los datos no deben ser transferidos a países fuera del espacio europeo, a menos que esos países garanticen un nivel adecuado de protección de los datos.

De la narración de los hechos contenidos en el numeral anterior, se observa que Google, con su accionar, violentó casi todos los principios, ya que el sujeto o interesado debe brindar su consentimiento al tratamiento, lo cual no ocurrió; tampoco se le comunicó que dicha información iba a ser recogida; hubo un procesamiento de una ingente cantidad de datos, y al ser transferidos a terceros, se generó una inseguridad sobre el tratamiento ilícito o no autorizado por éstos.

La segunda norma en discusión fue la relativa al derecho a reclamar daños, contenida en la sección 13, la cual regula los supuestos en que es procedente un reclamo y conforme a la cual, es necesario probar la existencia de una pérdida financiera o daño cuantificable, en cabeza del reclamante[24].

---

[23] En el Capítulo 2 titulado "Condiciones pertinentes a efectos del primer principio: tratamiento de cualquier dato personal", el numeral 1 exige que "El interesado ha dado su consentimiento al tratamiento".

[24] La sección en comento, a la letra, dice:
"(1) Una persona que sufre un daño debido a cualquier infracción por parte de un controlador de datos de cualquiera de los requisitos de esta Ley tiene derecho a una compensación del controlador de datos por ese daño.
(2) Una persona que sufre angustia debido a cualquier infracción por parte de un controlador de datos de cualquiera de los requisitos de esta Ley tiene derecho a una compensación del controlador de datos por esa angustia si:
(a) el individuo también sufre un daño a causa de la contravención, o
(b) la infracción se relaciona con el procesamiento de datos personales para fines especiales.

De su lectura se extrae que, conforme a la citada sección, cualquier individuo que sufra daños materiales, como resultado de alguna contravención a la norma, por parte de un controlador de datos, tiene derecho a recibir una compensación, siempre que lo demuestre y cuantifique. Por otra parte, el artículo limita el derecho a exigir indemnización por daños morales[25], ya que éstos solo serán reclamables cuando vienen acompañados de un daño material o cuando éstos fueron utilizados con fines especiales, los cuales, a tenor de lo establecido en el numeral tres, se refieren a fines periodísticos, artísticos o literarios.

1.3. La decisión y sus aspectos más relevantes

La sentencia fue dictada de manera unánime por los cinco jueces, quienes fallaron a favor de Google. De su lectura se desprende que los temas discutidos y analizados fueron, por una parte, la procedencia de las acciones colectivas en el ordenamiento jurídico del Reino Unido[26] en casos como el presente; y por la otra, el relativo a la necesidad de probar la ocurrencia de un daño –ya fuera material o moral, en los términos antes señalados– para que fuera procedente el reclamo, conforme a la normativa vigente para ese entonces, es decir la sección 13 de la Ley de Protección de Datos de 1998.

Con relación al tema adjetivo, vinculado con al análisis y procedencia de las acciones colectivas o *class actions*[27]*, la sentencia profundizó en este aspecto, ya que tal tipo de reclamos, que son comunes en otros países de sistema anglosajón* –como son los Estados Unidos y Canadá– no lo son en el Reino Unido. Sobre este particular sostuvo el juez que, la forma como fue presentada la demanda, es decir, un solo accionante erigiéndose como "representante" de todos los poseedores de un *IPhone* en Inglaterra y Gales para la fecha, sin demostrar el daño ocasionado (como sí fue en el caso de Vidal Hall V Google Inc.), así como exigiendo un monto uniforme para cada usuario por concepto de reparación o indemnización[28], fue en gran parte lo que conllevó a una decisión

(3) En los procedimientos iniciados contra una persona en virtud de esta sección, es una defensa demostrar que tuvo el cuidado que, en todas las circunstancias, era razonablemente necesario para cumplir con el requisito en cuestión." Traducción libre.

25 En los términos de la norma, "*distress*".

26 De acuerdo con la sentencia, conforme al derecho inglés existen tres tipos de acciones distintas, que pueden ser interpuestas por grupos de personas, denominadas *group actions*, *representative actions* y *collective proceeding,* siendo estas últimas un fenómeno reciente en el derecho inglés, (ver numeral 33 de la sentencia).

27 Ver el análisis contenido en los literales D) y E) de la sentencia.

28 La sentencia tuvo sus reservas sobre el monto reclamado por cada usuario ya que afirmó, en el Párrafo 87, citando un precedente que:
"La dificultad que enfrenta este enfoque es que el efecto de la solución alternativa de Safari obviamente no fue uniforme en toda la clase representada. No se impugnan ni podrían razonablemente impugnarse las conclusiones del juez, en [2018] EWHC 2599 (QB); [2019] 1 WLR 1265, párrafo 91, que:
'…algunos individuos afectados eran 'superusuarios', grandes usuarios de Internet. Habrán sido 'víctimas' de múltiples infracciones, con cantidades considerables de [información generada por el navegador] tomadas y utilizadas durante el Período Relevante. Otros habrán realizado muy poca actividad en Internet. A diferentes individuos se les habrá tomado

a favor de Google Inc. Se debe advertir que, la sentencia no desconoció el derecho que tenía el Sr., Lloyd de intentar una acción por daños y perjuicios a título personal, lo que discutió fue la opción procesal elegida. De haber sido este último el camino transitado por el demandante, probablemente la decisión hubiera sido otra[29].

De manera que la decisión pretendió establecer un límite a esas acciones colectivas, interpuestas por escritorios de abogados y financiadores de litigios, que, como señalamos, son comunes en los Estados Unidos pero no en el Reino Unido. No obstante, la decisión deja abierta la puerta para que acciones colectivas sean presentadas, siempre que un grupo de particulares afectados, puedan participar[30].

En lo referente al tema del daño, la sentencia sostuvo que la norma contenida en la Sección 13 de la Ley, aplicable para el momento de la ocurrencia de los hechos, exige dos requisitos concurrentes que se deben cumplir, para que el reclamo sea procedente:

En primer lugar, se debe proporcionar la evidencia del procesamiento ilegal de datos personales relacionados con un individuo determinado; y en segundo, lugar, se debe demostrar el daño material (por ejemplo, pérdida financiera) o moral, (angustia) que ha sido causado por el procesamiento ilegal de datos personales. La sentencia sostuvo que:

> "Esas palabras, sin embargo, no pueden interpretarse razonablemente en el sentido de que otorgan a una persona el derecho a una compensación sin prueba de daños o perjuicios materiales, cuando un controlador de datos comete una infracción

y utilizado diferentes tipos de información. En los documentos de reclamación se identifican no menos de 17 categorías de datos personales. Las categorías de datos especificadas varían en su sensibilidad, y algunas de ellas son 'datos personales sensibles' en el sentido de la sección 2 de la DPA (como la sexualidad o el origen étnico). … Pero no es creíble que Google haya obtenido todas las categorías de datos especificadas de cada demandante representado. … Los resultados de la adquisición y el uso también habrán variado según el individuo y sus actitudes hacia la adquisición, divulgación y uso de la información en cuestión".

[29] En el párrafo 23 de la sentencia, el juez expresó:
"No hay duda de que el demandante tiene derecho a presentar una demanda contra Google en su propio nombre, la cual tiene una perspectiva real de éxito. El problema es si también puede hacerlo en nombre de todos los demás usuarios de iPhone que caen dentro de la clase representada. Esto depende del alcance del procedimiento representativo disponible bajo las Reglas de Procedimiento Civil ('CPR'). Antes de llegar a ese procedimiento, mencionaré para compararlos los otros dos métodos de reclamar reparación colectiva actualmente disponibles en la ley procesal inglesa".

[30] En el párrafo 67 de la sentencia, el juez afirmó que:
"La producción en masa de bienes y la prestación en masa de servicios han tenido como resultado que, cuando se produce una conducta legalmente culpable, un grupo muy amplio de personas, en ocasiones millonarias, puede verse afectado. Como ilustra el presente caso, el desarrollo de tecnologías digitales se ha sumado al potencial de daño masivo por el cual se puede buscar reparación legal. En tales casos, es necesario conciliar, por un lado, la inconveniencia o la total impracticabilidad de litigar múltiples demandas individuales con, por otro lado, la inconveniencia o la total impracticabilidad de convertir a cada posible demandante (o demandado) en parte de una sola demanda. La única manera práctica de 'llegar a la justicia' es combinar los reclamos en un solo procedimiento y permitir que una o más personas representen a todos los demás que comparten el mismo interés en el resultado. Cuando no es factible juzgar todos los reclamos individuales, los adagios de Lord Eldon citados por Lord Macnaghten en Ellis siguen siendo tan pertinentes como siempre: que es mejor ir lo más lejos posible hacia la justicia que negarla por completo y que, si no puedes de manera realista, hacer que todos los interesados sean una parte, debe asegurarse de que aquellos que son partes 'intentarán lo correcto de manera justa y honesta'". Es lo que se ha denominado la acción de bifurcación en el Reino Unido". (Traducción libre).

> no trivial de cualquier requisito de la Ley, en relación con los datos personales de los que esa persona es el sujeto. En primer lugar, como se discutió anteriormente, la redacción de la sección 13 (1) establece una distinción entre 'daño' sufrido por un individuo y una 'infracción' de un requisito de la Ley por parte de un controlador de datos, y otorga un derecho a compensación 'por ese daño' sólo si el 'daño' ocurre 'en razón de' la contravención. Esta redacción es incompatible con un derecho a compensación basado únicamente en la prueba de la infracción. Decir, como hace la demandante en su escrito, que lo que se 'perjudica' es el derecho del interesado a que sus datos sean tratados de acuerdo con los requisitos de la Ley no cumple con este punto, pues equivale a reconocer que en el caso del demandante, el daño y la contravención son lo mismo[31]".

Sobre esta base, se sostuvo que la reclamación presentada por el Sr. Lloyd no podía prosperar y, estaba "condenada al fracaso"[32] ya que, para que se le otorgara una compensación en virtud de la Sección 13, el Sr. Lloyd tenía que haber demostrado que Google hizo un uso ilegal de los datos personales relacionados con cada individuo y que, como resultado de tal uso ilegal, el individuo sufrió algún daño[33].

Como se observa, el juez hizo una interpretación literal de la sección 13 de la ley vigente para el momento de los hechos, al sostener que, dada su redacción, la necesidad de probar los daños causados era un requisito indispensable para la procedencia de la acción. No obstante, la propia decisión deja claro que, como los hechos ocurrieron bajo la vigencia de la ley de 1998, quedaba fuera de análisis, la aplicación de la normativa vigente en este momento, es decir, la contenida en el Reglamento General de Protección de Datos[34] (RGPD)[35].

Cabría entonces preguntarse, cuál es actualmente la regulación en vigor bajo el marco del RGPD de la Unión Europea, tomando en cuenta que, ésta se ha erigido como modelo para las legislaciones de otras latitudes, tal como se verá en el siguiente numeral.

---

31 Párrafo 115 de la sentencia. (Traducción libre)

32 Párrafo 8 de la sentencia.

33 La decisión concluye, en el párrafo 138, sosteniendo que:
"Por todas estas razones, concluyo que el artículo 13 de la DPA de 1998 no puede ser razonablemente interpretada en el sentido de que confiere a un sujeto de datos el derecho a una compensación por cualquier contravención (no trivial) por parte de un controlador de datos de cualquiera de los requisitos de la Ley sin la necesidad de probar que la contravención ha causado daño material o angustia al individuo en cuestión". (Traducción libre).

34 La sentencia sostuvo, en el párrafo 16 que:
"Debido a que los actos y omisiones que dan lugar a la presente reclamación ocurrieron en 2011 y 2012, la reclamación se rige por la antigua ley contenida en la DPA 1998 y la Directiva de Protección de Datos. No obstante, las partes e intervinientes en sus presentaciones en este recurso hicieron frecuentes referencias a las disposiciones del Reglamento General de Protección de Datos y el DPA 2018. En principio, el significado y el efecto del DPA 1998 y la Directiva de Protección de Datos no pueden verse afectados por la legislación que ha sido promulgada posteriormente. Por tanto, la legislación posterior no puede ayudar a resolver las cuestiones planteadas en este recurso, y lo dejaré de lado". (Traducción libre).

35 También conocido por sus siglas en inglés GDPR (*General Data Protección Regulation).*

2. La regulación del reclamo por eventuales daños por los usuarios de redes sociales en el Reglamento General de Protección de Datos de la Unión Europea (UE)

El avance y crecimiento meteórico de las tecnológicas –que no conocen límites ni fronteras– ha hecho que las legislaciones de los estados se hagan insuficientes e inadecuadas para desarrollar una regulación efectiva. Paralelamente, ha ido desarrollándose una mayor conciencia sobre la importancia de los datos personales, como derecho fundamental del individuo, y la necesidad de que se dicten normas que protejan los derechos inherentes a éstos. Sin duda, ha sido la Unión Europea quien ha desarrollado la legislación más acabada en esta materia, que sirve de modelo para otras y que, al abarcar una amplísima extensión territorial y poblacional, se ha visto en la capacidad de poner coto a la desregulación existente.

En este contexto, es oportuno analizar si, a la luz de la normativa europea en vigor contenida en el RGPD[36], el caso en estudio hubiera tenido la misma decisión. La discusión gira fundamentalmente en si –bajo dicha norma– la sola pérdida de control de los datos por los usuarios, sin su consentimiento, acarrea o no el derecho a ser indemnizado, o se confirma la posición de la sentencia, que exige la existencia efectiva del daño.

La respuesta la encontramos en el artículo 82[37] que señala que:

> "1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.
> (…)
> 6. Las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el artículo 79, apartado 2".

La redacción de la norma es bastante escueta. De su interpretación literal pareciera que el reclamo por eventuales daños derivados de violaciones al Reglamento, de nuevo, está circunscrito a la prueba del daño, los cuales pueden abarcar muchos aspectos, como el mismo Reglamento enumera en sus considerandos[38].

---

[36] El Reglamento fue promulgado el 27 de abril de 2016, no obstante, tuvo una *vacatio legis* de más de dos años ya que, no fue sino hasta el 25 de mayo de 2018, que empezó a tener pleno vigor en todos los Estados miembros y con una prelación sobre la normativa nacional.

[37] Consultado en: http://data.europa.eu/eli/reg/2016/679/oj

[38] El considerando 75 enumera los daños y señala que, pueden tratarse de:
"Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse

Diversas opiniones habían surgido sobre el punto en discusión y, no fue sino hasta una sentencia, de reciente data dictada por la Sala Tercera del Tribunal de Justicia de la Unión Europea (TJUE), de fecha 4 de mayo de 2023[39], que se aclaró el contenido del articulado citado. Conforme a lo señalado por la decisión:

> "Por una parte, del tenor de esta disposición se desprende claramente que la existencia de «daños y perjuicios» o de «daños y perjuicios» que se han «sufrido» constituye uno de los requisitos del derecho a indemnización previsto en dicha disposición, al igual que la existencia de una infracción del RGPD y de una relación de causalidad entre dichos daños y perjuicios y esa infracción, de modo que estos tres requisitos son acumulativos.
>
> 33 Por lo tanto, no puede considerarse que toda «infracción» de las disposiciones del RGPD dé lugar, por sí sola, al referido derecho a una indemnización a favor del interesado, tal como se define en el artículo 4, punto 1, de dicho Reglamento.

al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados".

[39] Sentencia en el asunto C-300/21, UI v Österreichische Post AG.
El caso versó sobre una petición de interpretación prejudicial solicitada por la Corte Suprema de Austria en un litigio que llegó a ese tribunal, entre un ciudadano austríaco y Österreichische Post AG, (la agencia de correos de ese país).
Según lo que consta en la sentencia, la agencia de correos recogió información sobre las afinidades políticas de la población austriaca, a través de un algoritmo desarrollado que analizaba diversos criterios sociales y demográficos de sus usuarios y con esa información atribuyó a éstos una potencial afiliación política. Los datos así generados se vendieron a distintas organizaciones para permitirles realizar el envío de publicidad dirigida, todo ello sin haber informado a sus usuarios y mucho menos haber obtenido el consentimiento para dicho tratamiento. El caso es que a un ciudadano austríaco fue catalogado como partidario de extrema derecha, lo que "… le causó una importante contrariedad, una pérdida de confianza y un sentimiento de humillación", por lo que interpuso una acción contra la agencia de correos reclamando el monto de mil euros, como indemnización por los daños y perjuicios inmateriales que afirmaba haber sufrido. (párrafos 12 y 13 de la sentencia).
12 En el marco de su actividad, Österreichische Post trató datos que, mediante extrapolación estadística, la llevaron a inferir una elevada afinidad del demandante en el litigio principal con un determinado partido político austriaco. Estos elementos no fueron transmitidos a terceros, pero el demandante en el litigio principal, que no había consentido el tratamiento de sus datos personales, se sintió ofendido por el hecho de que se le hubiera atribuido afinidad con el partido en cuestión. La circunstancia de que se conservaran en el seno de la referida sociedad datos relativos a sus supuestas opiniones políticas le causó una importante contrariedad, una pérdida de confianza y un sentimiento de humillación. De la resolución de remisión se desprende que no se ha constatado ningún perjuicio distinto de estos daños temporales de carácter emocional.
en relación con el recurso interpuesto por el primero para obtener la reparación de los daños y perjuicios inmateriales que afirma haber sufrido como consecuencia del tratamiento por dicha sociedad de datos relativos a las afinidades políticas de personas residentes en Austria, en particular él mismo, cuando no había dado su consentimiento a tal tratamiento.
Consultada en:
https://curia.europa.eu/juris/document/document.jsf?docid=273284&doclang=ES

> Tal interpretación sería contraria al tenor del artículo 82, apartado 1, del citado Reglamento".

Se evidencia de su lectura que, en los términos de la jurisprudencia del TJUE, para la procedencia del reclamo o derecho a compensación previsto en el artículo 82 del RGPD, es necesario que concurran tres elementos acumulativamente: En primer lugar, que haya habido un tratamiento de datos personales llevado a cabo en violación de las disposiciones del RGPD, en segundo lugar se deberán demostrar los daños o perjuicios (materiales o inmateriales) sufridos por el sujeto de datos afectado y en tercer lugar, el vínculo causal entre el tratamiento ilícito y ese daño.

De manera que, el TJUE adopta, en materia resarcitoria, una postura intermedia, ya que, por una parte, no exige –para la procedencia del reclamo– la existencia de culpa del actor, pero por la otra, sí requiere demostrar la ocurrencia de algún daño, cualquiera que éste sea, que el reclamante haya sufrido, ya que, la sola realización de la conducta infractora no genera *per se* el derecho a exigir una indemnización.

Por lo que respecta específicamente al daño y su cuantía[40], la sentencia dejó establecido que la obligación de reparar abarca cualquier daño, sin importar su tamaño, de manera que ningún Estado miembro puede limitar la indemnización a un determinado umbral de gravedad[41].

El tema en análisis está en constante discusión y las soluciones pueden ser distintas según la jurisdicción donde se plantee el caso. Así, por ejemplo, en el Estado de Illinois en Estados Unidos, más de 1,4 millones de residentes han recibido a partir de mayo de este año, cheques por hasta 397 dólares, como compensación por una demanda colectiva de por 650 millones de dólares interpuesta contra Facebook en el año 2015, por el uso ilegal de datos de reconocimiento facial, mediante el cual los usuarios eran "invitados" a etiquetar a sus amigos en las fotos. Dicha demanda terminó en un acuerdo que fue refrendado por un juez y a partir de ese momento, la empresa modificó su sistema de etiquetado de fotos[42]. Por otra parte, en el Reino Unido, en abril de

---

[40] En el caso analizado, los tribunales austríacos habían desestimado la pretensión del demandante por considerar que el monto reclamado no superaba el umbral mínimo de daño indemnizable, tal como exige el derecho nacional austríaco.

[41] En el párrafo 46 dejó sentado que:
"En segundo lugar, el contexto en el que se inscribe esta disposición también indica que el derecho a indemnización no está supeditado a que los daños y perjuicios considerados alcancen un determinado umbral de gravedad. En efecto, el considerando 146 del RGPD establece, en su tercera frase, que «el concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia, de tal modo que se respeten plenamente los objetivos [de dicho] Reglamento». Pues bien, esta acepción amplia del concepto de «daños y perjuicios», propugnada por el legislador de la Unión, se vería contradicha si el referido concepto se limitara únicamente a los daños y perjuicios de cierta gravedad".

[42] Más información en: https://www.wsiltv.com/news/consumer/some-illinois-residents-receiving-397-checks-from-facebook-lawsuit/article_485b76ca-d764-11ec-a3bc-0b8c8830e3d6.html

2021, se interpuso una acción, en nombre de 3,5 millones de niños menores de 13 años, contra TikTok, por la recopilación ilegal de información personal de niños (incluidos números de teléfono, videos, datos de ubicación y datos biométricos), sin advertencia alguna y sin haber requerido los consentimientos necesarios de los padres ni informar sobre cómo se procesarían dichos datos personales. Tal juicio está en proceso.

3. La situación en Venezuela: Urge una normativa en protección de datos personales

Por último, no podemos dejar de hacer referencia a la inexistencia en Venezuela de una norma integral que regule la protección de datos personales[43]. Sobre el tema, sólo contamos con normas dispersas, como son la Constitución, la Ley Orgánica del Tribunal Supremo de Justicia[44], la Ley de Delitos Informáticos[45], la Ley de Infogobierno[46] y una sentencia de la Sala Constitucional del Tribunal Supremo de Justicia, de carácter vinculante, en la cual fijó los principios que deben cumplir, "... toda normativa o sistema sobre datos personales que contenga información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables"[47].

El caso que hemos revisado y sus implicaciones evidencia la insuficiencia de la normativa vigente y la urgente necesidad que existe de que el poder legislativo nacional dicte una norma completa que regule, conforme a los criterios internacionales imperantes, la protección de datos personales, así como políticas públicas que promuevan y defiendan estos derechos. Por supuesto, tal normativa conducirá a poner coto –tanto a las empresas como a los organismos públicos– en la obtención y uso no autorizado de datos personales de los ciudadanos[48]. Esa norma necesaria contribuirá a que nuestro país se reinserte en la esfera internacional[49].

---

43 Para un estudio sobre la normativa vigente, Zubillaga Marianela, "Recorrido por la normativa sobre protección de datos en la Unión Europea y la situación en Venezuela", Revista de Derecho Público, Nº 171-172, Julio Diciembre 2022, pág., 226.

44 Gaceta Oficial N° 6.684 Extraordinario del 19 de enero de 2022.

45 Gaceta Oficial Nº 37.313 del 30 de octubre de 2001.

46 Gaceta Oficial N° 40.274 del 17 de octubre de 2013.

47 Expediente Nº AA50-T-2004-2395. Consultada en: https://tugacetaoficial.com/jurisprudencia/jurisprudencia-vinculante-sobre-derecho-a-la-proteccion-de-datos-personales-en-venezuela/3/

48 En un artículo publicado en "La Voz de América" se afirma que: "Un informe revela que el acceso indebido a datos personales en Venezuela cuenta con recursos públicos y la incursión directa de entidades en las prácticas de robo de información, lo que indica la voluntad manifiesta del Estado en actividades ilícitas". Consultado en: https://www.vozdeamerica.com/a/venezuela-vulneracion-derecho-privacidad-proteccion-datos/6419822.html

49 En esta materia nos encontramos incluso por detrás de países como Cuba, quien en 2022, promulgó una norma. Así lo señala el informe elaborado por David Benisar, quien señala que:
"En 2022, hubo seis países que adoptaron leyes por primera vez: Indonesia, Cuba, Omán, Eswatini, Sri Lanka y Tanzania. Ahora hay 131 Estados Miembros de la ONU (2/3 de 193) que han adoptado leyes integrales de protección de datos. 20 jurisdicciones autónomas, incluyendo Taiwán, Kosovo y numerosos territorios de ultramar, también han adoptado leyes".

CONCLUSIONES

En el tema que nos ocupa, a nuestro juicio, estamos ante la discusión sobre varios extremos, por demás relevantes: Por un lado, si la sola infracción de la privacidad de los datos personales sin autorización se erige en sí misma, como una violación a un derecho fundamental que, de ocurrir, genera responsabilidad por parte del violador y derecho a una reparación, por parte de la víctima[50] o es necesario probar la entidad del daño causado. Ya el derecho europeo se ha pronunciado sobre ambos puntos. Veremos cómo lo harán otras jurisdicciones.

Otro aspecto a tomar en cuenta es que, la recopilación de datos personales por parte de las empresas tecnológicas sin autorización, se realiza con un fin y uso comercial y particularmente lucrativo, es decir, realizan una explotación comercial de dichos datos, que ha generado y genera a esas empresas cuantiosos beneficios, lo que podría implicaría una especie de aprovechamiento indebido de unos recursos –los datos personales– que pertenecen a otros y sobre los cuales, en principio, no tienen derecho. Es frente a estos extremos que los tribunales de los países deberán buscar un equilibrio, a los fines de, por una parte, impedir acciones temerarias por parte de fondos de reclamos o similares y por la otra, limitar que las empresas tecnológicas utilicen de manera masiva y sin autorización, datos de los usuarios de sus servicios, los almacenen, procesen y analicen y obtengan con ellos beneficios económicos.

Con la vigencia en Europa del RGPD, no existe duda alguna de que la recopilación de datos personales sin autorización constituye una violación a la normativa citada, basado en el carácter fundamental de la protección de datos como derecho autónomo y en el marco del derecho a la privacidad y la necesidad de proteger ambos derechos de manera efectiva. Tales violaciones acarrearán multas muy altas a ser impuestas por los organismos rectores en la materia. Ahora bien, según dicha normativa, la procedencia de una indemnización a favor de los ciudadanos se generará, siempre que dicha violación haya generado un daño, ya sea material o moral, que deberá probarse en los tribunales de instancia de los Estados miembros. Corresponderá al Tribunal de Justicia de la Unión Europea continuar delineando y circunscribiendo el ámbito de aplicación de dicha normativa, en los nuevos casos que se planteen en el futuro.

Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2023 (January 28, 2023). Consultado en: https://dx.doi.org/10.2139/ssrn.1951416

[50] Es decir, como un tipo de "responsabilidad objetiva" como ocurre en otras esferas del derecho, como es por ejemplo, la comisión de ciertas conductas anticompetitivas bajo la legislación de libre competencia, conforme a la cual, el solo despliegue de ciertas conductas acarrea la imposición de una sanción, independientemente de que se hayan generado daños o no al mercado relevante.

Por lo que respecta a Venezuela, si el país desea avanzar hacia la reinserción en la comunidad y comercio internacional, urge por una parte, la entrada en vigor de una ley que garantice la protección de los datos personales y por la otra, que dicha normativa cuente con los mecanismos eficientes que garanticen su efectividad y cumplimiento en todas las esferas de la vida, tanto pública como privada.

BIBLIOGRAFÍA

Banca y Negocios. (25 de mayo de 2022). Usuarios de Facebook en EEUU están recibiendo cheques de 397 dólares por violación de privacidad. Recuperado de https://www.bancaynegocios.com/usuarios-de-facebook-en-eeuu-estan-recibiendo-cheques-de-397-dolares-por-violacion-de-privacidad/

Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2023 (January 28, 2023). Recuperado de: https://ssrn.com/abstract=1951416 o http://dx.doi.org/10.2139/ssrn.1951416

Blanco, Luis Ernesto, "Dame tus «likes» para mentirte mejor", "*Debates IESA"*, [Internet], 16 octubre, 2018, consultado en: http://www.debatesiesa.com/dame-tus-likes-para-mentirte-mejor/

Bywater, André: "Vidal-Hall Data Protection Class Action Appeal Settled", Cordery Legal Compliance, [Internet], August 8, 2016, Recuperado de: https://www.corderycompliance.com/vidal-hall-data-protection-class-action-appeal-settled/

Comisión De La Unión Europea (UE), "La Construcción De Una Economía De Los Datos Europea", comunicación de la Comisión de la Unión Europea (UE) al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, [Internet], Bruselas, 10 de enero de 2017. consultado en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52017DC0009&from=EN#footnote2

Comisión De La Unión Europea (UE), "Una estrategia europea para los datos" comunicación de la Comisión de la Unión Europea (UE) al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, [Internet], Bruselas, 19 de febrero de 2020, Consultado en https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

Corte Suprema del Reino Unido, Lloyd v Google LLC [2021] UKSC 50 (10 de Noviembre de 2021), Recuperado de: https://www.bailii.org/uk/cases/UKSC/2021/50.html

Cuatrecasas. (2020, 7 de octubre). Indemnización de daños morales por infracción del RGPD. Cuatrecasas. https://www.cuatrecasas.com/es/spain/art/indemnizacion-de-danos-morales-por-infraccion-del-rgpd

El Economista. (2020). Big Data. Diccionario de Economía. https://www.eleconomista.es/diccionario-de-economia/big-data

Departamento de Protección al Consumidor de Connecticut. (2013, Noviembre 18). Connecticut, 36 Other States Reach $17M Settlement with Google. Recuperado de https://portal.ct.gov/DCP/News-Releases-from-the-Department-of-Consumer-Protection/2013-News-Releases/Connecticut-36-Other-States-Reach-17M-Settlement-with-Google

Ellerton Sam, What the Lloyd v Google mass data privacy case means for businesses, Lockton, [Internet], Recuperado de: https://global.lockton.com/gb/en/news-insights/what-the-lloyd-v-google-mass-data-privacy-case-means-for-businesses

El País, Cinco Días. (10 de agosto de 2012). Google tendrá que deshabilitar las "cookies espía" en Safari. Recuperado de: https://cincodias.elpais.com/cincodias/2012/08/10/empresas/1344765537_850215.html

Federal Trade Commission, "Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser", Recuperado de: https://www.ftc.gov/news-events/news/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented-privacy-assurances-users-apples

Finan, M. D., & McGrath, R. C. (s.f.). GDPR Article 82 – The CJEU Gives its First Judgment. consultado en: https://www.lawlibrary.ie/viewpoints/gdpr-article-82/

Frantziou, Eleni: *"Lloyd v Google: towards a more restrictive approach on privacy protection in the UK?", VerfBlog,* [Internet], 22 de noviembre de 2021, Recuperado de https://verfassungsblog.de/lloyd-privacy/, DOI: 10.17176/20211123-085055-0.

Gómez Muñoz, Xavier: "Y así llegamos a la era del retuit y el me gusta", *Revista Mundo Diners*. Dinediciones, [Internet], 1º de marzo de 2022, Recuperado de: https://revistamundodiners.com/la-era-del-retuit-y-el-me-gusta/

Herbert Smith Freehills. (10 de noviembre de 2021). Supreme Court finds claim for compensation under data protection legislation cannot proceed on `opt-out basis´ in high profile Lloyd v Google case. Recuperado de https://hsfnotes.com/litigation/2021/11/10/supreme-court-finds-claim-for-compensation-under-data-protection-legislation-cannot-proceed-on-opt-out-basis-in-high-profile-lloyd-v-google-case/

Hervada, B., Maneiro Dios, R., & Revesado Carballares, D. (2022). El aprendizaje cooperativo como estrategia para la enseñanza inclusiva. Papeles Salmantinos de Educación, (26), 261-279. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=6627893

La Vanguardia, [Internet], 25 de julio de 2019, "El creador del botón de retuit se arrepiente de su idea" consultado en: https://www.lavanguardia.com/tecnologia/actualidad/20190725/463690303652/ingeniero-responsable-boton-retweet-arrepiente.html#:~:text=Chris%20Wetherell%20fue%20el%20desarrollador,un%20ni%C3%B1o%20de%20cuatro%20a%C3%B1os

La Voz de América: Vulneración del derecho a la privacidad y protección de datos en Venezuela. https://www.vozdeamerica.com/a/venezuela-vulneracion-derecho-privacidad-proteccion-datos/6419822.html

Legislation.gov.uk. (s.f.). Data Protection Act 1998. Recuperado de https://www.legislation.gov.uk/ukpga/1998/29/contents

Llewellyn, A Tom: "Detailed review of Lloyd v Google: what does it mean and what next for claims management companies?" [Internet], 23 de noviembre de 2021, Recuperado de: https://www.rwkgoodman.com/info-hub/a-detailed-review-of-lloyd-v-google/#:~:text=The%20Supreme%20Court%20handed%20down,actual%20financial%20loss%20or%20distress.

News 3. (19 de mayo de 2022). Some Illinois residents receiving $397 checks from Facebook lawsuit. Recuperado de https://www.wsiltv.com/news/consumer/some-illinois-residents-receiving-397-checks-from-facebook-lawsuit/article_485b76ca-d764-11ec-a3bc-0b8c8830e3d6.html

Pang Angelina, "Lloyd v Google on Data Privacy Class Actions: Beginning of the End, End of the Beginning?", *LSE Law Review Blog*, [Internet], 15 de marzo de 2022, Recuperado de: https://blog.lselawreview.com/2022/03/lloyd-v-google-data-privacy-class-actions-beginning-end-end-beginning

Parlamento Europeo y del Consejo. (24 de octubre de 1995). Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, Diario Oficial L 281, 23/11/1995 P. 0031 – 0050. Recuperado de https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046

Parlamento Europeo y del Consejo. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Parker, N., & van der Leeuw-Veiksha, A. (11 de mayo de 2023). CJEU clarifies key aspects of the GDPR: an overview of recent cases. Allen & Overy. Recuperado de https://www.allenovery.com/en-gb/global/blogs/data-hub/cjeu-clarifies-key-aspects-of-the-gdpr-an-overview-of-recent-cases

Privacy Helper. (s.f.). Data Protection Act 1998 - A Summary of the 8 Guiding Principles. Recuperado de https://www.privacyhelper.co.uk/knowledge-hub-articles/data-protection-act-1998-a-summary-of-the-8-guiding-principles

Rayón, Álex: "La economía del dato: retos y oportunidades", *Business Review* (Núm. 256) TIC, [Internet], Mayo 2016, [Internet], Recuperado de: https://www.harvard-deusto.com/la-economia-del-dato-retos-y-oportunidades

Reino Unido. (s.f.). Guidance Note B2: Data Protection Act 1998 & Access to Personal Data. Recuperado de https://assets.publishing.service.gov.uk/media/5a790500e5274a277e691436/B220090423MOD_FOI_Guidance_DPA_and_personal_infoU.pdf

Reuters. (27 de Agosto de 2022). Meta's Facebook agrees to settle data privacy lawsuit. Recuperado de https://www.reuters.com/legal/metas-facebook-agrees-settle-data-privacy-lawsuit-2022-08-26/

Revista Seguridad - UNAM. (s.f.). Leyes de protección de datos personales en el mundo y la protección de datos biométricos. Recuperado de https://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93

Smith, Alex: "Lloyd -v- Google: a landmark decision" 23 de noviembre d3 2021, Hiil Dickson. [Internet], Recuperado de: https://www.hilldickinson.com/insights/articles/lloyd-v-google-landmark-decision

Vidal-Hall and others v Google Inc (Information Commissioner intervening). (2015). Court of Appeal. Recuperado de https://www.ucpi.org.uk/wp-content/uploads/2018/03/Vidal-Hall-v-Google-Inc-Information-Commissioner-intervening-2015-EWCA-Civ-311-2016-QB-1003.pdf

Tribunal de Justicia de la Unión Europea, Sala Tres. Caso: ECLI:EU:C:2023:62. Comisión Europea contra República de Polonia, párrafos 1-3, 15 de marzo de 2023.Recuperado de:

https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=4960697.

Voz de América. (2022, Enero 31). Vulneración del derecho a la privacidad y protección de datos en Venezuela. Recuperado de https://www.vozdeamerica.com/a/venezuela-vulneracion-derecho-privacidad-proteccion-datos/6419822.html

Zubillaga Marianela, "Recorrido por la normativa sobre protección de datos en la Unión Europea y la situación en Venezuela", *Revista de Derecho Público*, Nº 171-172, Julio Diciembre 2022, pág., 226.