DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

"NATURALEZA INTRÍNSECA", "CONTEXTO" O "FINALIDAD" EN LA DETERMINACIÓN DEL CARÁCTER SENSIBLE DE LOS DATOS PERSONALES

"INTRINSIC NATURE", "CONTEXT" OR "PURPOSE" IN THE DETERMINATION OF THE SENSITIVE CHARACTER OF PERSONAL DATA

*Julio A. Huerta Anguiano**

RESUMEN. El presente artículo expone tres posibles respuestas a la pregunta de investigación siguiente: ¿qué hace que los datos personales sean considerados datos personales sensibles? Esta aportación tiene como objetivo contribuir a la revisión crítica del concepto de "datos personales sensibles" o "categorías especiales de datos", destacando algunos de los problemas implícitos en la construcción e interpretación de su definición jurídica, teniendo como marco de referencia diversos ordenamientos internacionales de protección de datos personales. En particular, el texto analiza los enfoques siguientes: 1) la concepción de la naturaleza *intrínsecamente sensible* de los datos personales; 2) la aproximación del carácter sensible en función del contexto de su procesamiento, y 3) la propuesta que considera la finalidad del tratamiento de los datos personales.

PALABRAS CLAVE. Datos personales, datos sensibles, categorías especiales de datos, privacidad, autodeterminación informativa.

* Licenciado y maestro en derecho por la Facultad de Derecho de la UNAM. Maestro en derecho norteamericano por la Universidad de Notre Dame (EE. UU.). Ex becario Fulbright – García Robles para estudios de posgrado. Abogado de protección de datos personales y privacidad. *juliohanguiano@gmail.com*.

Fecha de recepción: 24 de junio de 2019.
Fecha de dictamen: 28 de octubre de 2019.

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

ABSTRACT. This article explains three possible answers to the following research question: why is some personal information considered as sensitive personal data? This paper aims to contribute to the critical review of the concept of "sensitive personal data" or "special data categories". It highlights some of the problems implied in the construction and interpretation of its legal definition, considering various international data protection laws. In particular, this text analyzes the following three approaches: 1) the conception of the intrinsically sensitive nature of personal data; 2) the approach of the sensitive character according to its context of processing; and 3) the thesis that considers the purpose of data processing.

KEYWORDS. Personal data, sensitive data, special categories of data, privacy, informational self-determination.

I. Introducción

Diversos cuestionamientos surgen cuando se analiza una definición de datos personales sensibles; por ejemplo: ¿es posible establecer un catálogo de datos personales sensibles que sea exhaustivo?; en todos los casos, ¿los datos que aparecen en una definición de este tipo son datos que puedan afectar los derechos y las libertades de sus titulares?; ¿puede haber otros datos que, aun sin estar incluidos en una definición, deban ser considerados sensibles en función del contexto o la finalidad de su tratamiento?; ¿a quién debe reconocérsele la facultad de determinar el carácter sensible de la información?, ¿al legislador?, ¿a las autoridades de control o protección de datos personales cuando deciden sobre un caso específico?, ¿a las cortes y tribunales cuando emiten sentencias o criterios?, ¿al mismo titular de los datos personales?

Las respuestas a estas interrogantes no son evidentes; por el contrario, estas cuestiones convierten a la definición de datos personales sensibles en una de las definiciones más obscuras para cualquier operador jurídico que tenga a su cargo una labor de interpretación y aplicación de normas de protección de datos personales.

En esta aportación se pretende contribuir a la difusión de algunas de las posturas planteadas en Europa desde hace varios años —pero que hoy en día continúan siendo poco conocidas en los países de Latinoamérica— respecto a la consideración del carácter *a priori* de los datos personales sensibles, así como a la importancia de la finalidad y el contexto del tratamiento en la determinación de su estatus sensible.

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

La difusión de estas ideas podría beneficiar a los Estados latinoamericanos y a los mismos destinatarios de las normas de protección de datos, en la medida que constituyen enfoques que podrían ser tomados en cuenta para orientar reformas legislativas futuras, y para fomentar una interpretación amplia (extensiva e incluyente) del concepto que vaya más allá de la aplicación estricta de una definición jurídica que prevea categorías expresas de datos sensibles.

Antes de entrar al tema, es importante mencionar que la definición estándar de "datos personales" los concibe como "cualquier información concerniente a una persona física identificada o que pueda ser identificada a través de medios que puedan ser razonablemente utilizados". Esta definición ha sido incluida en diversos ordenamientos internacionales de protección de datos personales.[1] Paralelamente al concepto de datos personales, ha surgido el concepto de "datos personales sensibles" o "especialmente protegidos". La idea de que algunos tipos de información son más sensibles que otros ha sido articulada a menudo por especialistas en privacidad, y reconocida por legisladores bajo una gran diversidad de términos (Etzioni, 2015: 1277). Sobre el particular, existen investigaciones que demuestran que el concepto de datos sensibles es considerado uno de los núcleos centrales de la privacidad y la protección de datos (Wang y Jiang, 2017: 3286).

La distinción entre datos personales sensibles y no sensibles es fundamental porque reconoce que el procesamiento de datos personales puede tener distintos niveles de impacto en la vida privada de las personas, así como en diversos valores protegidos por el derecho. La dicotomía presupone que el tratamiento de cierto tipo de información puede implicar riesgos y afectaciones importantes para sus derechos y libertades fundamentales. Así lo expone el autor Sabah Al-Fedaghi, para quien la sensibilidad de los datos personales es uno de los factores más importantes para determinar la percepción de privacidad de un individuo, reconociendo que el grado de sensibilidad influye en la decisión sobre el nivel de seguridad que se establece para controlar el acceso a dicha información (Al-Fedaghi, 2007).

Diversos son los autores que han destacado el papel de la "dignidad humana" como norma sustantiva básica y fundamento de los derechos huma-

[1] En las Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) que regulan la protección de la privacidad y el flujo transfronterizo de datos personales (artículo 1[b]); en el Convenio 108 del Consejo de Europa (artículo 2[a]); en los Estándares Internacionales sobre Protección de Datos Personales y Privacidad (apartado 2[a]); en la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (artículo 2[a]), y más recientemente, en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, que deroga la Directiva 95/46/CE (artículo 4[1]).

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

nos (Neal, 2014: 31; Carozza, 2008: 932), así como la importancia de la privacidad como un valor que protege la autonomía de las personas (Gavison, 1980: 423). Teniendo en cuenta que muchas legislaciones han reconocido al derecho a la protección de las personas físicas respecto al tratamiento de sus datos personales como un derecho fundamental, sea de manera expresa en sus Constituciones o a través de la adopción de criterios por parte de sus tribunales, puede reconocerse que la regulación de los datos sensibles también busca proteger valores esenciales, tales como la no discriminación (Žliobaitė y Custers, 2016: 185), la dignidad de los individuos, y el libre desarrollo de la personalidad(Wang y Jiang, 2017: 3290).

Uno de los orígenes más conocidos acerca de los datos personales sensibles se remonta a las Directrices de la OCDE, que regulan la protección de la privacidad y el flujo transfronterizo de datos personales (OCDE, 1980). Si bien la versión final de este documento no incluyó una definición de datos sensibles, su Memorando Explicativo refirió que la ausencia de una definición de datos personales sensibles se debió a la falta de consenso sobre qué categorías de datos merecían una especial protección. Según consta en los numerales 19(a) y 51 del Memorando, en las Directrices de la OCDE ya se había advertido que quizá no era posible adoptar una serie de datos que fuesen considerados universalmente como sensibles.

Caso distinto fue el Convenio 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal (Council of Europe, 1981a), el cual sí incluyó una serie de medidas y controles para el tratamiento de las denominadas "categorías particulares de datos". Concretamente, este ordenamiento dispuso en su artículo 6o. que los datos de carácter personal que revelaran el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podían tratarse automáticamente a menos que el derecho interno de los Estados proporcionara garantías apropiadas para tal fin. Lo mismo aplicaría tratándose de datos personales relativos a condenas penales.

Asimismo, el Reporte Explicativo del Convenio 108 estableció, en sus numerales 44 y 45, respecto al alcance del artículo 6o. del Convenio, que la expresión "revelen ...opiniones políticas, religiosas y otras creencias" cubría también las actividades provenientes de tales opiniones o convicciones, y que los datos personales relativos a la salud incluían la información concerniente a la salud pasada, presente y futura, física y mental, de un individuo. Esta información podía referirse a una persona enferma, sana o fallecida, e incluía aquellos relacionados con el abuso del alcohol o el consumo de drogas.

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

Por otra parte, el Reporte Explicativo refirió, en su numeral 48, que la lista de datos que conformaban las categorías especiales establecidas en el artículo 6o. del Convenio 108 no eran exhaustivas, y, por tanto, que un Estado contratante podía, de conformidad con el artículo 11 del propio Convenio, incluir en su derecho interno categorías adicionales de datos personales sensibles.

El 14 de diciembre de 1990, la Asamblea General de la Organización de las Naciones Unidas (ONU) adoptó los Principios Rectores para la Reglamentación de los Ficheros Computarizados de Datos Personales de las Naciones Unidas (ONU, 1990), cuyo artículo relativo al "principio de no discriminación" estableció la prohibición de registrar datos que pudieran originar una discriminación ilícita o arbitraria, en particular información sobre el origen racial o étnico, color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo, o sobre la participación en una asociación o la afiliación a un sindicato.

En un sentido similar, la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Parlamento Europeo y Consejo de la Unión Europea, 1995), estableció en su artículo 8(1) que los Estados miembros debían prohibir el tratamiento de los datos personales que revelaran el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad de las personas.

Posteriormente, los Estándares Internacionales sobre Protección de Datos Personales y Privacidad (Autoridades de Protección de Datos y Privacidad, 2009) establecieron, en su apartado 13, una definición de datos personales sensibles, que los concibió como aquellos datos de carácter personal que afecten a la esfera más íntima del interesado, o cuya utilización indebida pueda dar origen a una discriminación ilegal o arbitraria, o conllevar un riesgo grave para el interesado. En particular, se consideran sensibles en la Resolución de Madrid los que puedan revelar aspectos como el origen racial o étnico, las opiniones políticas, convicciones religiosas o filosóficas, así como los datos relativos a la salud o a la sexualidad.

De manera más reciente, el Reglamento General de Protección de Datos de la Unión Europea (RGPD, 2016), que deroga la Directiva 95/46/CE, dispuso en su artículo 9(1), bajo el rubro "categorías especiales de datos personales", que quedaba prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física. El siguiente cuadro incluye los tipos o categorías que han sido tradicionalmente considerados como datos sensibles (contiene las categorías que aparecen textualmente como datos personales sensibles en los ordenamientos de referencia).

Categorías específicas	*Directrices de la OCDE (1980)*	*Convenio 108 (1981)*	*Resolución ONU 45/95 (1990)*	*Directiva 95/46/CE (1995)*	*Resolución de Madrid (2009)*	*LFPDPPP (2010) y LGPDPPSO (2017)*	*Reglamento General UE (2016)*
	Datos que revelen:						
Origen racial o étnico		X	X	X	X	X	X
Opiniones políticas		X	X	X	X	X	X
Convicciones o creencias religiosas		X	X	X	X	X	X
Convicciones filosóficas			X	X	X	X	X
Estado de salud		X		X	X	X	X
Sexualidad o vida sexual		X	X	X	X		X
Orientación sexual							X
Pertenencia o afiliación a sindicatos			X	X		X	X
Datos genéticos						X	X
Datos biométricos							X
Condenas penales		X		X			X
Creencias de otro tipo		X	X			X (Creencias morales)	

FUENTE: elaboración propia con base en la búsqueda y revisión de los ordenamientos jurídicos respectivos.

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

El panorama anterior constituye únicamente un punto de partida para contextualizar algunos de los problemas implícitos en la construcción e interpretación del concepto de datos personales sensibles. Si bien esta reflexión es de carácter general, se considera que es trasladable a distintos ordenamientos en la medida que los problemas expuestos son, en gran parte, inherentes al "lenguaje natural" que conforma cualquier norma jurídica.

A menudo, el concepto de datos personales sensibles parte de una definición jurídica con rango de norma general y abstracta que le confiere obligatoriedad. De conformidad con el *Cambridge Dictionary of Philosophy*, una "definición" puede concebirse como la especificación de un significado o la especificación del contenido conceptual de una expresión. Por otra parte, recordando a Norberto Bobbio, se consideran normas generales cuando se refiere a normas que se dirigen a una clase de personas, y normas abstractas cuando son aquellas que regulan una acción-tipo (o una clase de acciones) (Bobbio, 2007: 133).

El elemento que detona la operatividad práctica del concepto de "datos sensibles" en el derecho positivo es una definición jurídica, destinada a regular la conducta de personas físicas o jurídicas de carácter público o privado (responsables del tratamiento) que deciden sobre acciones específicas de procesamiento (obtención, uso, divulgación, conservación, entre otros). Una vez que una definición de este tipo ha sido establecida y aprobada por el legislador, se constituye como un referente normativo imperativo. Lo anterior de ninguna manera implica que no pueda establecerse una relación entre el concepto de datos sensibles y otros valores fundamentales, tales como la dignidad humana y la no discriminación, e inclusive encontrar una justificación suficiente en ellos. No obstante, por cuestiones de espacio, el estudio de estas relaciones básicas no será objeto de la presente aportación.

Las definiciones de "datos personales" sensibles a menudo incluyen categorías expresas a las cuales el legislador ha decidido otorgarles un mayor nivel de protección. Sin embargo, aunque pudiera pensarse que estas definiciones proporcionan una guía clara y bien definida a los intérpretes de la norma (responsables del tratamiento, oficiales de privacidad, abogados de protección de datos personales, entre otros), la interpretación y aplicación de la definición de "datos sensibles" implica diversos problemas.

Una primera cuestión es que algunas legislaciones incluyen supuestos normativos muy amplios, enunciados como: son datos sensibles "aquellos que afecten la esfera más íntima de una persona", "cuya utilización indebida pueda dar origen a una discriminación ilegal o arbitraria", o bien,

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

"aquellos que conlleven un riesgo grave para el interesado o el titular de los datos".[2]

Cuando existe una norma jurídica que define los términos contenidos en las disposiciones, o bien, existe algún criterio orientador de una corte o tribunal, la vaguedad o ambigüedad de los conceptos tiende a disminuir. No obstante, en muchos sistemas jurídicos no existe una conexión manifiesta entre las hipótesis generales previstas en la definición y los subtipos que podrían vincularse o asociarse a las mismas, haciendo más difícil distinguir entre información sensible e información no sensible; dificultando consecuentemente el cumplimiento de la regulación en la materia.

Históricamente, los ordenamientos de protección de datos han privilegiado categorías expresas de datos sensibles respecto a la determinación casuística de cuándo se afecta la "esfera más íntima" de una persona (esto requeriría definir previamente el ámbito de la "intimidad"); o determinar la actualización de un "riesgo grave" para el titular o interesado (¿qué tan grave debería ser el riesgo para que un dato se considere sensible?), o el surgimiento de una situación de "discriminación ilegal o arbitraria" derivada de una utilización indebida de la información (¿causar discriminación debe ser el objetivo del tratamiento, o bastaría con que ésta apareciera en cualquier momento del tratamiento?, ¿quién determina que existe una situación de discriminación?).

Aunque, en efecto, un enfoque de manejo de riesgos es actualmente considerado una herramienta esencial para asegurar una protección adecuada de las personas en relación con el tratamiento de sus datos personales, por ejemplo, en el contexto del RGPD (Gellert, 2018: 279), parece más intuitivo aplicar categorías expresas de datos que identificar riesgos específicos.

La cuestión anterior conduce a otro punto que no es menos problemático. Se trata justamente de la remisión a categorías aparentemente más concretas. Esta especificidad es sólo superficial, debido a que es altamente probable que las categorías expresas no refieran de manera detallada todos los subtipos de información que pueden ubicarse dentro de ellas. Por

[2] Ordenamientos que contienen este doble aspecto son los Estándares Internacionales de Protección de Datos (apartado 13 [1]); las leyes federales de protección de datos personales mexicanas (Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2010: artículo 3[VII]; Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017: artículo 3[X]); la Ley por la cual se dictan disposiciones generales para la protección de datos personales de Colombia (Ley Estatutaria 1581, 2012: artículo 5o.), y la Ley sobre protección de vida privada de Chile (Ley 19628, 1999: artículo 2[g]), por citar algunos casos.

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

ejemplo, pensar en términos de "género" y "especie". La tipología de datos personales sensibles prevista en una definición constituiría el género, pero sus especies serían el resultado de individualizar y derivar datos más particulares a partir de la tipología general.

En diversos informes jurídicos, la Agencia Española de Protección de Datos (AEPD) ha analizado la naturaleza de diversos datos no previstos expresamente en la legislación de la materia, para concluir si debían ser considerados datos especialmente protegidos o no. Es el caso de los datos que revelan "aspectos psicológicos" de personas físicas (AEPD, 1999); el carácter del dato de profesión de "sacerdote" (AEPD, 2004a); la información personal relativa a un determinado servicio de prevención de riesgos laborales (AEPD, 2004b); la condición de ser fumador (AEPD, 2005); las historias clínicas de personas fallecidas (AEPD, 2008), entre muchos otros.

Lo anterior es relevante debido a que en muchos casos no existe un referente normativo claro en la reglamentación específica que pueda orientar la determinación del carácter sensible de los datos personales. Por lo tanto, la existencia de una definición de "datos sensibles" sólo es el punto de partida para una labor de análisis, interpretación y reconstrucción de significados, cuyos parámetros no siempre están manifiestamente establecidos.

II. Enfoques sobre el carácter sensible de los datos personales

1. *Los datos personales sensibles y su naturaleza "intrínsecamente sensible"*

La concepción de la naturaleza "intrínsecamente sensible" de los datos personales sostiene que este tipo de información posee cualidades específicas inherentes, distintas a otro tipo de información, que potencializan un riesgo para las personas físicas, particularmente haciendo posible una afectación a sus derechos y libertades una vez que se encuentran sujetos a un tratamiento. En este sentido, esta postura defiende la idea de que los datos personales son sensibles independientemente de cualquier contexto o del reconocimiento que haga una norma jurídica específica.

Sin embargo, la alusión a la naturaleza sensible de los datos personales debe ser matizada y ubicada en contexto para evitar algunas confusiones. Sobre este punto, resulta de utilidad señalar que el término "naturaleza"

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

denota comúnmente a una esencia inherente, inmutable y necesaria, relativa a los aspectos físicos de la realidad, por contraste con algo que es contingente o circunstancial. Por ejemplo, la naturaleza del agua es el resultado de la composición química de dos átomos de hidrógeno y uno de oxígeno (H_2O) (en todos los casos, la naturaleza del agua es la composición de estos elementos). En consideración a la connotación del término, parece dudoso que podamos hablar de una naturaleza similar cuando hablamos del concepto de "datos personales sensibles" y sus categorías.

Adoptar una posición como la anterior representaría defender una actitud esencialista, en la cual un dato personal posee una misma naturaleza sensible, independientemente de cualquier norma jurídica o valoración humana e independientemente de cualquier uso específico. En un extremo, podría afirmarse conforme a este enfoque que ciertas categorías poseen en sí mismas un peso *ontológico*, un peso que es intrínsecamente mayor al de otro tipo de información personal; por ejemplo, sostener que las fotografías de personas físicas son en sí mismas sensibles, o afirmar que el peso y la altura de una persona deberían ser siempre datos especialmente protegidos. Por otra parte, es plausible apuntar que una interpretación estricta de esta postura podría conducir a dejar fuera del concepto, información íntima que pudiera ser empleada para causar un daño o afectación significativa a las personas, por no haber sido categorizada como información sensible de manera expresa.

En este sentido, es posible cuestionar si las opiniones políticas o los datos que reflejan aspectos como origen racial o étnico son datos necesariamente (y no accidentalmente) sensibles, y, por tanto, datos que afectan la esfera "más íntima de su titular"; o bien, considerar que los datos que revelan opiniones políticas o convicciones religiosas son "por naturaleza" más sensibles que la información que revela el patrimonio económico, ubicación geográfica en tiempo real o historial de navegación en Internet de una persona física. Esto, sin duda, es discutible.

Muchas legislaciones no consideran a los datos de geolocalización y los historiales de búsqueda en Internet como información sensible. No obstante, parece razonable afirmar que estos datos permiten inferir conclusiones muy precisas respecto a la vida privada de las personas a quienes concierne la información. Al respecto, diversos tribunales y organismos han señalado que los datos de geolocalización permiten derivar hábitos precisos de la vida cotidiana, lugares de residencia permanentes o temporales, movimientos diarios u otras actividades llevadas a cabo por las personas, haciendo posible inferir tipos de relaciones e intereses, así como los entornos sociales frecuentados por ellos.

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

En *United States v. Jones*, un caso histórico analizado por la Suprema Corte de los Estados Unidos de Norteamérica, la *Justice* Sonia Sotomayor manifestó, en su opinión concurrente, que el monitoreo por sistema de posicionamiento global (GPS), incluso por un periodo corto de tiempo, permite generar un registro preciso y completo de los movimientos públicos de una persona, y que ello refleja una gran cantidad de detalles sobre sus asociaciones familiares, políticas, profesionales, religiosas y sexuales. La *Justice* Sotomayor argumentó que muchos datos obtenidos por GPS tienen una naturaleza indiscutiblemente privada, tales como información que revela viajes al psiquiatra, al cirujano plástico, a la clínica de abortos, al centro de tratamiento del SIDA, al club de *striptease*, al abogado defensor, al motel, a la reunión sindical, a la mezquita, la sinagoga o la iglesia, entre otros (*United States v. Jones*, 2012).

En un sentido similar, el Comité Europeo de Protección de Datos[3] (EDPB, por sus siglas en inglés) ha expuesto que los metadatos y los datos de tráfico y ubicación proporcionan medios para establecer un perfil de las personas a quienes conciernen, información que no es menos sensible que el contenido de las comunicaciones, teniendo en cuenta el derecho a la privacidad (EDPB, 2018: 12).

En el caso de los historiales de navegación, también ha cobrado mayor fuerza, en los últimos años, el argumento de que revelar este tipo de información podría comunicar situaciones íntimas o información que las personas desean mantener como confidencial (desde las noticias que leen, los sitios web de compras que visitan, o los sitios para adultos que frecuentan), lo cual podría perjudicar la percepción que la sociedad tiene de un individuo, afectando su reputación en su vida profesional o en su vida pública. Este debate se suscitó hace un par de años en la Unión Americana, a partir de unas reglas emitidas por la Federal Communications Commission (FCC) que proponían obligar a los proveedores de servicios de telecomunicaciones a obtener el consentimiento expreso de las personas antes de comunicar o compartir los historiales de búsqueda en la red. La FCC definió el historial de navegación web y el historial de uso de aplicaciones como información sensible, junto con otro tipo de información, tales como los datos de ubicación geográfica, la información financiera y de salud, así

[3] Anteriormente llamado Grupo de Trabajo del artículo 29, creado en virtud del artículo 29 de la Directiva 95/46/CE. Se trataba de un organismo europeo con carácter consultivo e independiente para la protección de datos y el derecho a la intimidad. Sus funciones se describían en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE. Con la entrada en vigor del RGPD, el Grupo de Trabajo cambió su denominación por la de Comité Europeo de Protección de Datos (*European Data ProtectionBoard*).

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

como el contenido de las comunicaciones (FCC, 2016: 4). Las reglas finalmente fueron repelidas por el presidente Donald Trump en 2017.

También se podría cuestionar si los datos que revelan opiniones filosóficas o políticas son sensibles para todos los individuos, pues seguramente existen personas para quienes poco importe que sus creencias morales y convicciones filosóficas o políticas sean conocidas o difundidas públicamente. Todas estas cuestiones deben ser evaluadas de manera cuidadosa, ya que podrían entrar en juego factores adicionales que, en efecto, puedan llevar a reafirmar el carácter de este tipo de información como sensible.

Hace casi veinte años, el profesor Spiros Simitis advirtió que muchas leyes de protección de datos personales consideraban la enumeración de datos sensibles como exhaustiva, y que era perceptible la creencia de que el atributo "sensible" estaba reservado a una clase exclusiva de datos cuidadosamente seleccionados e incluidos por los legisladores. Simitis criticó esta postura. En su opinión, la intervención del legislador en el establecimiento de categorías fijas tenía (como tiene actualmente) una función estratégica: garantizar el máximo de transparencia y estabilidad posible al ordenamiento correspondiente, protegiéndolo de demasiados cambios, y sujetando su modificación únicamente al proceso legislativo formal (Simitis, 1999: 3).

Sobre el particular, es pertinente reconocer que parte de la función de una definición de "datos personales sensibles" es establecer qué información requiere, *prima facie*, un cuidado y manejo especial cuando es tratada por personas físicas o jurídicas, autoridades, servicios u otros organismos públicos o privados, en consideración a las consecuencias negativas que pudieran derivarse para los derechos y libertades de los titulares de la información a partir de su tratamiento. No obstante, esta generalización es en parte tendenciosa, en la medida que asume que, en una sociedad determinada, los datos personales "x", "y" y "z" son considerados por todos los individuos con el mismo carácter "sensible", o que el tratamiento de dichos datos implica, en todos los casos y para todos los individuos, un nivel de riesgo o afectación similar en su tratamiento.

En relación con lo anterior, una cosa es que ciertas categorías de datos estén contempladas en una definición jurídica como datos sensibles, y otra que dichas categorías sean consideradas sensibles por los titulares de los datos personales. A partir del reconocimiento de una norma jurídica que establezca una definición de datos sensibles, no se sigue necesariamente la creación de un riesgo concreto, o un estado mental en el cual las personas asuman ciertas categorías de datos como merecedoras de especial cuidado en sus vidas.

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

Además, con el desarrollo vertiginoso de las tecnologías de la información y la comunicación; la velocidad con la que viaja la información a través de la red; la sofisticación de los medios electrónicos para la obtención, uso y explotación de la información; el desarrollo de avances en las áreas de inteligencia artificial (IA), minería de datos y *Big data* (entre otros), y ante la falta de una cultura adecuada sobre el uso de los datos personales por parte de responsables y titulares, entre otros factores, cualquier dato o conjunto de datos personales podría convertirse en información sensible en cualquier momento, aunque no se encuentren previstos de manera expresa en una definición.

Particular atención requieren los recientes dispositivos y aplicaciones que incorporan IA, los cuales pueden requerir para su desarrollo u operación del procesamiento de grandes cantidades de datos personales, impactando potencialmente en los derechos a la privacidad y la protección de datos personales de las personas, generando nuevos riesgos potenciales que son inducidos por la tendencia a la concentración masiva de datos personales. Esta situación fue reconocida en la Declaración sobre Ética y Protección de Datos en la Inteligencia Artificial, adoptada en la 40a. Conferencia Internacional de Comisionados de Protección de Datos y Privacidad el 25 de octubre de 2018 (ICDPPC, por sus siglas en inglés) (ICDPPC, 2018).

Ahora bien, la concepción de la naturaleza intrínsecamente sensible encuentra una variante mucho más moderada en la determinación *a priori* del carácter sensible de los datos personales, la cual si bien no considera que los datos personales son sensibles en sí mismos, sí afirma que las categorías de datos tienen un carácter sensible como regla general, y con anterioridad a su aplicación práctica. Los defensores de este enfoque apriorístico (en mayor o menor medida) también suelen llevar a cabo una interpretación estricta de la definición, desproveyendo a la información de un contexto particular respecto a su uso y las consecuencias de su tratamiento. Para ellos, se trata de partir del carácter sensible anterior o predeterminado de las categorías previstas en la definición, para proceder a aplicarlas de manera *cuasi-mecánica* a los datos en cuestión.

Como aporte al análisis está el ejemplo presentado por Rebecca Wong respecto a la publicación de una fotografía de un esquimal. La pregunta que realiza la autora recae sobre si la publicación de esta información podría considerarse como tratamiento de datos personales sensibles por revelar el origen racial de la persona retratada. En opinión de la autora, la prohibición de tratar datos personales sensibles contenida en el artículo

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

8(1) de la hoy abrogada Directiva 95/46/CE, habría sido aplicable sin importar qué tan trivial hubiese sido el caso (Wong, 2007: 9).

De manera similar, es posible referir la sentencia del *Caso Bodil Lindqvist* (Sentencia C-101/01, 2003), adoptada por el Tribunal de Justicia de las Comunidades Europeas (TJCE) el 6 de noviembre de 2003, el cual tuvo su origen en diversas cuestiones prejudiciales sobre la interpretación de la Directiva 95/46/CE, planteadas al TCJE por el *Götahovrätt* sueco, en el marco de un proceso penal en contra de una mujer acusada de haber infringido la normatividad sueca de protección de datos personales, al publicar en su sitio de Internet, diversos datos de carácter personal sobre varias personas.

En particular, Lindqvist había publicado en Internet el nombre, trabajo, pasatiempos, números de teléfono, circunstancias familiares, entre otra información personal de sus compañeros que, como ella, colaboraban voluntariamente en una parroquia de la Iglesia protestante de Suecia, sin haberles informado sobre la existencia de la página web y sin haber solicitado el consentimiento para proceder al tratamiento de sus datos.

Es de interés la cuestión prejudicial que versa sobre el hecho de si conforme al artículo 8(1) de la Directiva 95/46/CE, la divulgación en un sitio web de la circunstancia de que un compañero de trabajo (designado por su nombre en el sitio web) se había lesionado el pie y estaba en una situación de baja temporal, constituía un dato relativo a la salud (y por tanto un dato especialmente protegido). A esta interrogante, el Tribunal respondió afirmativamente, señalando que era preciso dar una interpretación amplia a la expresión "datos relativos a la salud", de modo que comprendiera la información relativa a todos los aspectos, tanto físicos como psíquicos, de la salud de una persona.

Las implicaciones del *Caso Lindqvist* son significativas, en la medida que en la "interpretación amplia" realizada por el Tribunal subyace una inferencia realizada a partir de la asociación de conceptos semejantes; por ejemplo, relacionar el concepto amplio de salud (la información que revela aspectos físicos y psíquicos de una persona) con los elementos "lesión", "miembro del cuerpo", "baja temporal", "persona física", sin tener en cuenta un análisis de por qué en el caso específico, de manera adicional a lo dispuesto por el artículo 8(1) de la Directiva 95/46/CE, la indicación de que una persona se ha lesionado un pie y está en una situación de baja parcial representaba algún riesgo a los derechos o libertades de su titular, a efecto de considerarlo un dato especialmente protegido. Es cierto que esta cuestión no fue presentada al Tribunal; sin embargo, en la sentencia emitida en el *Caso Lindqvist* no se advierten elementos que permitan concluir que

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

el contexto del tratamiento tenía un papel importante en la determinación del carácter especialmente protegido de la información referida.

2. *Datos personales sensibles en función del contexto de su tratamiento*

Este enfoque, también conocido como *context-based approach*, sostiene que es el contexto del tratamiento el que confiere a los mismos una cualidad particular casuística y específica. Para Helen Nissenbaum, el término "contexto" se refiere a entornos sociales estructurados con características que han evolucionado con el tiempo y están sujetos a una serie de causas y contingencias de propósito, lugar, cultura, historia y más (Nissenbaum, 2010: 130). Conforme a un enfoque contextual, cualquier dato personal puede, dependiendo de las circunstancias de su tratamiento, adquirir el carácter sensible.

En un sentido similar se pronuncian Simitis y McCullagh, para quienes la naturaleza especial de los datos personales sensibles no deriva necesariamente de la aplicación de las categorías previstas en la definición, sino del caso concreto del tratamiento, en el cual se considere, por ejemplo, las características de la persona titular de los datos, las condiciones de lugar, tiempo y modo en las que se lleve a cabo el tratamiento, el grado de exposición o divulgación de la información, el nivel de riesgo en función del dato personal, las posibles consecuencias que se derivarían de un posible uso indebido en la esfera de los derechos del titular o interesado, entre otros (Simitis, 1999: 5; McCullagh, 2007: 11 y 12).

Esta aproximación es visible en el RGPD, cuyo considerando 51 dispone que "[e]special protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales…" (RGPD, 2016).

Como puede advertirse, en el diseño del RGP el legislador europeo matizó el alcance a la expresión "naturaleza", al referir expresamente al contexto del tratamiento que puede dar surgimiento a diversos riesgos para los derechos y las libertades fundamentales de los individuos.

Desde hace muchos años, el legislador europeo resaltó la importancia de las circunstancias específicas en las que los datos personales son tratados para considerarlos especialmente protegidos. En este aspecto, se podría traer a cuenta lo dispuesto en el artículo 6(43) del Reporte explicativo del

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

Convenio 108, el cual enfatiza que el riesgo de que el tratamiento de datos personales sea dañino para las personas generalmente no depende del contenido de los datos, sino del contexto en el que son procesados.

A partir de este enfoque, en efecto puede haber casos donde el tratamiento de ciertas categorías de datos conduzca a la intrusión de derechos e intereses individuales. Sin embargo, justamente debido a que la determinación de cierto tipo de información como datos personales sensibles es contextual, no existirían parámetros o criterios que, de manera universal, puedan ser aplicados para determinar su carácter sensible. Sin duda, esto representa un gran problema, ya que fuera de los elementos proporcionados por la propia definición (categorías generales), la ausencia de criterios conduce necesariamente a una interpretación diferente y especifica en cada caso, una interpretación en la cual un mismo dato personal podría tener un carácter sensible y no sensible dependiendo del contexto.

Este problema era visible en la categorización de datos personales sensibles prevista en la Directiva 95/46/CE, la cual resultaba problemática en la práctica. Por citar un caso: el 20 de abril de 2011, Jacob Kohnstamm —en representación del entonces Grupo de Trabajo del Artículo 29 (Grupo de Trabajo)— envió una carta a Françoise le Bail, directora general de la Comisión Europea, refiriéndose a un comunicado previo en el que se requería a este organismo europeo una opinión acerca de algunas prácticas identificadas a nivel nacional relacionadas con problemas en la implementación de la Directiva 95/46/CE (Article 29 Working Party, 2011a).

Entre los diversos cuestionamientos, la carta solicitaba al Grupo de Trabajo sugerencias de mejora o cambios en relación con la implementación a nivel nacional del artículo 8o. de la Directiva 95/46/CE sobre las categorías especiales de datos, y valorar si era necesario revisar las categorías de los datos considerados sensibles y sus excepciones.

Consecuentemente, el Grupo de Trabajo emitió el documento denominado *Advice paper on special categories of data ("sensitive data")*, en el cual analizó algunos de los problemas existentes en la aplicación del artículo 8o. de la Directiva 95/46/CE. En este documento, el Grupo de Trabajo destacó algunas ventajas y desventajas del enfoque basado en categorías expresas, así como del enfoque que tiene en cuenta el contexto del tratamiento para la determinación del carácter sensible de los datos, cuestionándose si la aproximación al enfoque de los datos sensibles debía revisarse con el objetivo de incrementar la flexibilidad del concepto (Article 29 Working Party, 2011b).

Sobre el enfoque adoptado en la Directiva 95/46/CE, el Grupo de Trabajo manifestó como aspecto positivo el envío de una fuerte señal política

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

a los Estados de que el procesamiento de datos sensibles se encuentra, por regla general, prohibido. También resaltó como ventaja la existencia de un alto grado de armonización en cuanto a las categorías de datos sensibles previstas en el artículo 8(1), lo cual proporcionaba seguridad jurídica a los responsables del tratamiento en cuanto a la aplicación de dichas categorías. No obstante, este organismo identificó como desventaja el hecho de que una lista cerrada de categorías era inflexible e incapaz de reaccionar al contexto del tratamiento, así como a las nuevas formas de procesamiento que podían ocurrir en el curso de los desarrollos tecnológicos.

En opinión del Grupo de Trabajo, a través del enfoque contextual puede otorgarse protección a nuevas formas de procesamiento y categorías de datos personales, las cuales podrían ocurrir a la luz de nuevos desarrollos tecnológicos. No obstante, este grupo consultivo también reconoció algunas desventajas, entre ellas las diferencias que surgirían en las legislaciones nacionales sobre posibles categorías adicionales de datos personales sensibles, así como la incertidumbre jurídica para los responsables del tratamiento respecto de dichas categorías, incluyendo la gran variedad de excepciones que podrían incluirse a su tratamiento en las legislaciones de implementación correspondientes.

Este último punto conduce de nueva cuenta a considerar que, en una gran mayoría de casos, se esperaría que la norma jurídica incluyese de manera específica los parámetros para favorecer su aplicación. No obstante, esta situación conllevaría el riesgo de excluir elementos extra normativos importantes para orientar el cumplimiento. Al menos como una hipótesis probable, podría incurrirse en el uso excesivo de una interpretación formalista de las categorías que conforman la definición de "datos sensibles", trayendo como consecuencia que la información personal fuese desprovista de un contexto adecuado, relevante o significativo; una situación poco deseable para los partidarios que defienden la "interpretación contextual" en la definición del carácter sensible de los datos personales.

Es importante aclarar que la crítica presentada no se formula en contra del establecimiento de una definición que haga referencia a ciertos datos como especialmente protegidos, sino en contra de adoptar una clasificación expresa y cerrada de datos personales a los que se les otorgue el carácter sensible, asumiendo que los mismos poseen tal propiedad en cualquier supuesto. Ciertamente, es posible identificar datos personales que en una generalidad de condiciones puedan considerarse sensibles, pero en la medida que una misma información personal es susceptible de ser sometida a varios tratamientos para fines diversos, también es plausible que su carácter sensible varíe en cuestión de grado, llegando inclusive al punto en que

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

los datos que se creían originalmente sensibles pierdan tal carácter al ser tratados en un contexto completamente distinto.

Llama la atención lo expresado por el Grupo de Trabajo en el documento sobre categorías especiales de datos personales, debido a que parece implicar que si bien cada Estado tiene discrecionalidad para ampliar las categorías de datos sensibles de acuerdo con el contexto particular, las nuevas categorías deberían quedar reconocidas nuevamente, de manera explícita, en una definición jurídica o en alguna otra parte del ordenamiento jurídico. Precisamente, este reconocimiento expreso es parte del problema, ya que elevar nuevas categorías a una definición podría conducir a incurrir de nueva cuenta en la situación que se pretende evitar; esto es, descontextualizar las categorías de datos sensibles volviéndolas estáticas en una definición. En ese sentido, considerando que el contexto de un tratamiento es comúnmente dinámico, no estático, al ser determinadas contextualmente, las nuevas categorías no deberían ser fijas o permanentes, sino flexibles.

Además, debe tomarse en cuenta que el enfoque contextual podría resultar incompatible con las categorías adoptadas en una definición cerrada de datos personales sensibles, ya que es posible identificar datos personales que aun siendo considerados sensibles por una definición, dado el contexto de su tratamiento, representen un riesgo o impacto menor en la esfera de derechos y libertades de los titulares. Por el contrario, información no considerada sensible por una definición jurídica podría adquirir tal carácter en un momento posterior, conduciendo a los intérpretes de la norma a adoptar medidas más estrictas para su tratamiento.

Por último, es importante señalar que el enfoque contextual es perfectamente compatible con la ausencia de una definición expresa de datos sensibles, ya que los mismos podrían determinarse caso por caso. Esto, sin embargo, aumentaría el grado de incertidumbre, convirtiendo al concepto en un concepto altamente subjetivo.

3. *Datos personales sensibles en función de la finalidad de su tratamiento*

Conforme a este enfoque, también denominado *purpose-based approach*, el componente "sensible" se detona cuando subyace al tratamiento de datos personales una finalidad de ocasionar un "daño o aflicción" a una persona física, o bien, cuando la finalidad en sí misma es revelar información sensible (McCullagh, 2007: 12 y 13; ICO, 2011: 8).

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

Actualmente, aunque no existe un claro consenso respecto a la definición de los términos "contexto" y "finalidad" en la protección de datos personales, su relación se considera innegable. Así lo señala Maximilian von Grafenstein, quien expone que los expertos en derecho, así como las autoridades de protección de datos, a menudo usan estos términos de manera intercambiable, sin precisar las diferencias en su significado. Para Von Grafenstein, el contexto de un tratamiento de datos incluye la finalidad de su procesamiento, y esta finalidad caracteriza, junto con otras circunstancias, el contexto correspondiente (Von Grafenstein, 2018: 104 y 105).

En su estudio sobre el principio de finalidad, este autor hace referencia a la sentencia sobre la Ley del Censo del 15 de diciembre de 1983, emitida por el Tribunal Constitucional de la República Federal de Alemania. Según cita este autor, en esta sentencia el Tribunal elaboró el primer enfoque para relacionar los términos "contexto" y "finalidad". Con el objetivo de determinar el alcance del derecho a la autodeterminación informativa, el Tribunal sostuvo que no únicamente era necesario examinar los tipos de datos proporcionados, sino examinar las posibilidades de su uso. Esto dependía, por una parte, del propósito de la recolección de los datos (finalidad), y por otra, de las posibilidades de las técnicas específicas de tratamiento y de la combinación de los datos. Considerados de manera conjunta, finalidad, técnicas de tratamiento y combinación de los datos, darían como resultado el contexto del tratamiento (Von Grafenstein, 2018: 101).

Teniendo en cuenta que actualmente el tratamiento de los datos personales tiene lugar en ambientes altamente descentralizados y no lineales —por ejemplo, tratamientos en la nube (King y Raja, 2012: 309)—, en donde es posible efectuar diversas operaciones de tratamiento de manera paralela o simultánea, existe una relación fundamental entre las circunstancias en las cuales surge el tratamiento de datos personales y las finalidades que subyacen al mismo. En el transcurso del tiempo pueden surgir diversos contextos de tratamiento, y también diversas finalidades que predeterminen estos contextos (Von Grafenstein, 2018: 105).

En este sentido, la pregunta es: ¿cómo distinguir diferentes finalidades y contextos en un tratamiento de datos personales que hagan posible la determinación del carácter sensible de los datos? Dicho de otro modo, ¿cuáles contextos y finalidades, evaluados de manera conjunta, podrían ser jurídicamente relevantes para determinar el carácter sensible de los datos? Las respuestas a estas interrogantes aún esperan ser desarrolladas satisfactoriamente.

Diversas leyes de protección de datos han incluido definiciones de "datos sensibles" como datos que "revelen" o puedan "revelar" determinados

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

aspectos de las personas físicas, tales como el origen étnico o racial, opiniones políticas, creencias religiosas o filosóficas, entre otras. La Real Academia Española define el término "revelar" como el hecho de "descubrir o manifestar lo ignorado o secreto", o bien, "proporcionar indicios o certidumbre de algo". En este sentido, una posible interpretación de "revelar" se traduciría en el hecho de hacer visibles o patentes los aspectos íntimos o privados de una persona, los cuales se encuentran ocultos o secretos, y únicamente son conocidos por la persona misma. Esta manifestación podría realizarse proporcionando indicios o diversos grados de certidumbre sobre dichos aspectos relativos a la "intimidad" o "privacidad", información que únicamente a una persona corresponde controlar de manera libre, específica e informada.

Como una construcción conceptual, el componente "revelar" tiene sentido; sin embargo, llevarlo a la práctica del derecho a la protección de datos personales trae consigo diversos problemas. Esta situación fue expuesta por la autoridad de control de protección de datos del Reino Unido, el Information Commissioner's Office (ICO), en el documento *Proposed new EU General Data Protection Regulation: Article-by-article análisis paper*, en el cual, como su nombre lo indica, examinó artículo por artículo la propuesta del RGPD y expresó, respecto al artículo 9(1) que no era claro lo que la expresión "revelar" significaba en la definición de las categorías especiales de datos personales (ICO, 2013: 11).

De manera similar al ejemplo planteado por Wong respecto a la publicación de una fotografía de un esquimal (Wong, 2007: 9), el ICO cuestionó si una fotografía de una persona de raza negra revelaba su origen étnico, y, por tanto, si debía ser considerada un dato personal sensible. Sobre el particular, el ICO consideró que dicha fotografía podía ser considerada un dato sensible si el propósito o finalidad del tratamiento era precisamente "analizar" o "revelar" (en el sentido de exponer a otros) el origen racial o étnico de la persona, y no el simple hecho de que una fotografía revelase circunstancialmente diversa información acerca de un individuo (ICO, 2013: 11).

Es interesante destacar que desde 2011, el ICO propuso que se adoptara una definición que considerara los efectos adversos o discriminatorios en individuos, grupos de personas o en la sociedad en general. En opinión de este organismo, cualquier definición futura de datos sensibles debía considerar si el tratamiento de la información tenía el potencial de causar a los individuos un daño significativo o alguna especie de aflicción. La postura del ICO se inclinó a determinar el carácter sensible de los datos

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

teniendo en cuenta el contexto y el riesgo al que estaría expuesta la persona (ICO, 2011: 8).

Y en efecto, podría preguntarse si todas las fotografías deben ser consideradas datos personales sensibles por el simple hecho de que exponen ciertos rasgos o características físicas de las personas. Esta postura parece no ser convincente para el ICO, quien ha tenido reservas acerca de aceptar el concepto general (no contextual) de las categorías de datos sensibles, privilegiando, por el contrario, una postura más flexible a favor de que la "sensibilidad" de la información refleja, en la medida de lo posible, la concepción promedio de los ciudadanos sobre lo que es considerado por ellos con tal carácter. Sin embargo, este organismo tiene en cuenta que adoptar categorías expresas de datos especialmente protegidos es parte de la corriente europea y que es poco probable que sea abandonada (ICO, 2013: 12).

La posición del ICO también parece sugerir que los intérpretes de las normas de protección de datos deberían tener en cuenta tanto la finalidad de quien lleva a cabo el tratamiento de los datos personales sensibles como el contexto en el que surge dicho tratamiento, incluyendo la evaluación del riesgo que representa para los titulares de los datos, el tratamiento de la información que les concierne.

Sobre este punto, actualmente muchos expertos reconocen que la función de las leyes de protección de datos es fungir como mecanismos para regular "riesgos" originados por el tratamiento de datos personales. Christopher Kuner *et al*. expresan que la gestión de riesgos es una herramienta crítica para garantizar que los datos se procesan adecuadamente, y que los derechos fundamentales de los individuos sean protegidos efectivamente (Kuner *et al*., 2015: 95).

Los autores señalan que utilizar un método de gestión de riesgos es la forma más eficiente para asegurar la objetividad y relevancia de las acciones a realizar al configurar un tratamiento de datos personales. Además, consideran que existe un acuerdo creciente en considerar que las leyes de protección de datos personales deben proteger a las personas físicas en contra de amenazas, riesgos y daños, incluyendo no únicamente los impactos tangibles (como los daños físicos o financieros), sino también los intangibles, así como daños más amplios para la sociedad general (Kuner *et al*., 2015: 97).

Un enfoque similar se advierte en el RGPD, cuyo artículo 35 impone la obligación de elaborar una Evaluación de Impacto en la Protección de Datos Personales, cuando el tratamiento de los datos pueda derivar en un riesgo alto para los derechos y libertades de los titulares, particularmen-

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

te en los derechos a la privacidad y protección de datos, aunque también podría involucrar a las libertades de expresión, pensamiento, movimiento, derecho a la no discriminación, así como a las libertades de conciencia y religión (Article 29 Working Party, 2017).

Sin embargo, las opiniones difieren respecto al estándar para medir los riesgos. Algunos abogan por la necesidad de elaborar una categorización de las formas de daño mediante descriptores, en tanto que otros consideran que el estatus de la protección de datos como derecho fundamental hace esta determinación inherentemente subjetiva (Kuner *et al*., 2015: 97).

Desde hace muchos años han surgido críticas que consideran que probablemente no sea posible establecer una serie de datos que sean universalmente considerados como sensibles. Esta aproximación refleja el hecho de que no todos los datos personales merecen categóricamente ser objeto de protección como información sensible, sino que la protección apropiada depende, como se ha señalado anteriormente, del contexto y de la finalidad con la cual los datos personales son tratados.

En 2011, en la respuesta proporcionada a un comunicado elaborado por la Comisión Europea, el ICO admitió que la categorización de datos personales sensibles era un área que no funcionaba bien en la práctica, y que las categorías previstas en la Directiva 95/46/CE probablemente no coincidían con lo que los individuos consideraban "sensible" en sus vidas (ICO, 2011: 6).

Por ejemplo, el ICO reconoció que la información relativa a la afiliación sindical había sido usada en los regímenes totalitarios de Europa en contra de grupos de personas o individuos específicos. Sin embargo, la autoridad de control del Reino Unido señaló que diversos miembros de sindicatos que viven actualmente en sociedades relativamente estables y democráticas podrían no considerar la información relativa a la afiliación sindical como información sensible, debido a que no se sienten expuestos a alguna amenaza en particular, a pesar de que esta información hubiese sido empleada indebidamente en el pasado. Por el contrario, actualmente, muchas personas podrían considerar la información acerca de sus finanzas o ubicación geográfica como información mucho más sensible (ICO, 2011: 6).

De esta manera, el ICO planteó que puede existir, con alto grado de probabilidad, una falta de correspondencia entre lo que la ley estipula y lo que la gente considera sensible en una sociedad determinada. Por lo tanto, el problema al definir una lista de categorías de información sensible es que dichas categorías son establecidas a partir de un juicio basado enteramente en costumbres sociales o culturales en un tiempo determinado. En opinión de este organismo, esta situación podía llevar a ciertas catego-

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

rías de datos que, de otro modo, podrían considerarse sensibles, a quedar fuera de la definición.

Particularmente este texto comparte el punto de vista del ICO y apoya la idea de que la regulación de los datos sensibles debería reflejar un reconocimiento de los intereses, preferencias, apreciaciones y opiniones que en una sociedad existen respecto a qué información los individuos consideran como especialmente sensible. Y es aquí donde se podría elaborar más el argumento, señalando que actualmente cualquier dato o información podría constituirse como información sensible, teniendo en cuenta no únicamente el contexto del tratamiento, sino la percepción de cada uno de los individuos. Un argumento como el anterior fue elaborado por William Parent en su artículo "Privacy, Morality, and the Law" (Parent, 1983).

William Parent fue uno de los precursores de lo que se conoce actualmente, en diversos países que adoptan la tradición jurídica del *common law*, como *Information privacy law* o *Data privacy law*, un área del derecho anglosajón que guarda enormes similitudes (con algunos matices y diferencias) con el derecho de protección de datos personales continental. Aunque las ideas y aportaciones de Parent fueron desarrolladas en el contexto del *common law* de los Estados Unidos de América, muchas de sus distinciones conceptuales continúan vigentes y son en extremo útiles para comprender algunos de los problemas actuales en temas de privacidad y protección de datos personales, incluso en países de tradición del derecho civil.

De acuerdo con este autor, la información personal consiste en hechos que la mayoría de las personas en una sociedad determinada eligen no revelar sobre sí mismos (excepto a amigos cercanos, familiares, entre otros); o hechos sobre los cuales un individuo es particular o fuertemente sensible y que, por tanto, elige no revelar a otros, aunque a la mayoría de las personas no les importe si estos mismos hechos son ampliamente conocidos acerca de ellos (Parent, 1983).

Trasladando la tesis de Parent al presente análisis, la adopción de una definición de datos sensibles, aunque orientadora y con pretensiones de ser general, es compatible con que cada persona establezca su escala de valores o jerarquías respecto a qué tipo de información merecería una mayor protección y cuidado. En efecto, las personas podrían considerar irrelevantes o inexactas las categorías previstas en la definición por no ajustarse a sus intereses, preferencias o expectativas personales. En tal caso, existiría una discrepancia entre lo que la norma establece y lo que los destinatarios de la misma consideran y protegen en sus vidas como información sensible.

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

Aunque Parent no aborda de manera directa el tema de la protección de datos personales, su definición es compatible con la existencia de información sensible, la cual depende de una apreciación de la persona, basada en una decisión subjetiva que se traduce en no revelar información que para ella es delicada o muy sensible. Así entendido el concepto, es posible imaginar diversos aspectos, situaciones, características y hábitos que cada persona desea mantener lejos del conocimiento público, o bien, sobre los cuales desearía ejercer un control más estricto. Conforme a esta postura, la adopción de una definición de datos sensibles pudiera ser innecesaria, además de ser más arbitraria y circunstancial de lo que pudiera pensarse, pues la apreciación personal basada en el poder de decisión de una persona autónoma y libre fundamentaría la "sensibilidad" de la información.

En este sentido, se asume como un presupuesto válido que cada individuo posee una escala de valores respecto de la información que considera debería protegerse con mayor cuidado, y por tanto, que desearía mantener alejada del conocimiento público, así como de tratamientos específicos. Esto, sin embargo, trae consigo el problema de convertir la valoración y determinación del carácter especialmente protegido de cierta información en una decisión altamente subjetiva.

La adopción de una definición de "datos personales sensibles" parece ser necesaria para orientar el cumplimiento de las normas de protección de datos. Sin embargo, una interpretación restringida y "mecánica" de la definición debería evitarse, ya que esta situación podría desproveer a los datos personales en cuestión de un contexto adecuado y relevante que permita adoptar una postura respecto de su carácter sensible. Asimismo, teniendo en cuenta que cuantas más posibilidades de uso tengan los datos recabados, más ambiguo (y peligroso) se vuelve el proceso de tratamiento de éstos, por lo que debería privilegiarse una interpretación amplia de los datos personales, con el objetivo de proporcionar una protección más extensa a los titulares de los datos personales.

III. Conclusión

En el texto se ha expuesto que el carácter especialmente protegido de cierto tipo de información personal deriva, en gran parte, del reconocimiento que hace el ordenamiento jurídico. Sobre este punto se ha apuntado que los datos personales carecen de una esencia o naturaleza *intrínsecamente sensible*. En ese sentido, esta concepción debe adoptarse de forma mesurada, ya que su interpretación estricta podría convertir una definición que debería

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

ser flexible en una definición de ornamento poco razonable en la práctica debido a su rigidez y falta de correspondencia con una realidad específica.

Para determinar la protección especial de los datos personales sensibles debería considerarse el contexto y la finalidad de su tratamiento. En este sentido, se ha señalado la posibilidad de que, con motivo de la evaluación del contexto y la finalidad del tratamiento, pueda considerarse sensible la información no prevista inicialmente en las categorías expresamente reconocidas por una definición jurídica de datos sensibles. De la misma manera, una evaluación del contexto y la finalidad también podría conducir a considerar menor el impacto de las consecuencias derivadas del tratamiento de los datos considerados especialmente protegidos en los derechos y libertades de las personas.

Asimismo, se ha compartido la idea de que las categorías o tipos de datos personales incluidos en una definición de datos personales sensibles no deberían ser consideradas exhaustivas, sino únicamente orientadoras, dejando abierta la posibilidad de que se incorporen nuevas categorías de datos que reflejen efectivamente lo que los miembros de una sociedad definan como información sensible en un tiempo determinado. Detrás de esta última afirmación se encuentra la posibilidad de que exista una falta de correspondencia entre las categorías previstas en una definición de datos personales sensibles, y lo que las personas titulares de los datos consideran como información sensible en sus vidas.

Históricamente, el concepto de los datos personales sensibles ha sido un tema desafiante que ha abierto la puerta a numerosos debates respecto a su construcción e interpretación. Las opiniones vertidas en esta aportación pretenden constituirse únicamente como un punto de partida para reflexiones y estudios futuros en Latinoamérica. La definición del concepto de "datos personales sensibles" es, sin duda, una de las figuras que ha generado y seguirá generando innumerables controversias y discusiones sobre su interpretación y aplicación.

Finalmente, si bien el sistema jurídico no podría operar en el ámbito de la subjetividad —o bien, definiendo de manera interminable categorías de datos personales sensibles—, sí es posible extender la interpretación del concepto, favoreciendo una interpretación más garantista del derecho fundamental a la protección de las personas físicas respecto al tratamiento de sus datos personales. La labor pendiente es justamente desarrollar una metodología que permita expandir el concepto para cubrir nuevas categorías de datos personales, así como definir parámetros que permitan evaluar la razonabilidad práctica de excluir categorías previstas en la definición cuando su aplicación conduzca a conclusiones triviales.

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

IV. Bibliografía

Al-Fedaghi, Sabah, 2007, "How sensitive is your personal information?", en *Proceedings of the 2007 ACM Symposium on Applied Computing*, Nueva York, NY: Association for Computing.

Bobbio, Norberto, 2007, *Teoría general del derecho*, 3a. ed., Colombia, Temis.

Carozza, Paolo G., 2008, "Human Dignity and Judicial Interpretation of Human Rights: A Reply", *The European Journal of International Law,* vol. 19, núm. 5, disponible en: *https://academic.oup.com/ejil/article/19/5/931/505548*.

Etzioni, Amitai, 2015, "A cyber age privacy doctrine: More coherent, less subjective, and operational", *Brooklyn Law Review*, vol. 80, núm. 4, disponible en: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2506313*.

Gavison, Ruth, 1980, "Privacy and the Limits of Law", *Yale Law Journal*, vol. 89, núm. 3, disponible en: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957*.

Gellert, Raphaël, 2018, "Understanding the notion of risk in the General Data Protection Regulation", *Computer Law & Security Review*, vol. 34, Issue 2, disponible en: *https://doi.org/10.1016/j.clsr.2017.12.003*.

King, Nancy J. y Raja, V. T., 2012, "Protecting the privacy and security of sensitive customer data in the cloud", *Computer Law & Security Review*, vol. 28, disponible en: *https://doi.org/10.1016/j.clsr.2012.03.003*.

Kuner, Christopher *et al*., 2015, "Risk management in data protection", *International Data Privacy Law*, vol. 5, Issue 2, mayo, disponible en: *https://academic.oup.com/idpl/article/5/2/95/645238*.

Mccullagh, Karen, 2007, "Data sensitivity: proposals for resolving the conundrum", *International Commercial Law and Technology,* vol. 2, núm. 4, disponible en: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1378121*.

Neal, Mary, 2014, "Respect for human dignity as «substantive basic norm»", *International Journal of Law in Context*, vol. 10, Issue 1, disponible en: *https://doi.org/10.1017/S1744552313000359*.

Nissenbaum, Helen, 2010, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford California, Stanford University Press.

Parent, William A., 1983, "Privacy, morality, and the law", *Philosophy and Public Affairs*, vol. 12, núm. 4, disponible en: *https://www.jstor.org/stable/2265374?seq=1/analyze*.

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

Simitis, Spiros, 1999, *Revisiting Sensitive Data*, Consejo de Europa, disponible en: *https://rm.coe.int/09000016806845af*.

Von Grafenstein, Maximilian, 2018, *The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation*, Baden-Baden, Alemania, Nomos Verlagsgesellschaft *mb,* disponible en: *https://www.jstor.org/stable/j.ctv941v5w.4?seq=44#metadata_info_tab_contents*.

Wang, Min y Jiang, Zuosu, 2017, "The Defining Approaches and Practical Paradox of Sensitive Data: An Investigation of Data Protection Laws in 92 Countries and Regions and 200 Data Breaches in the World", *International Journal of Communication*, vol. 11.

Wong, Rebecca, 2007, "Alternative Approaches to Sensitive Data?", *Journal of International Commercial Law and Technology*, vol. 2, núm. 1, disponible en: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=936391*.

Žliobaitė, Indrė y Custers, Bart, 2016, "Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models", *Artificial Intelligence and Law*, vol. 24, Issue 2, disponible en: *https://doi.org/10.1007/s10506-016-9182-5*.

1. *Documentos de trabajo y sentencias*

Agencia Española de Protección de Datos, 2008, *Datos de salud de personas fallecidas*, Informe Jurídico 0149/2008, disponible en: *https://www.aepd.es/es/documento/2008-0149.pdf*.

Agencia Española de Protección de Datos, 2005, *Naturaleza del dato de fumador como dato de salud,* Informe 0129/2005, disponible en: *https://www.aepd.es/es/documento/2005-0129.pdf*.

Agencia Española de Protección de Datos, 2004a, *Carácter del dato de profesión de sacerdote*, Informe 44/2004, disponible en: *https://www.aepd.es/es/documento/2004-0044.pdf*.

Agencia Española de Protección de Datos, 2004b, *Tratamiento conforme a la legislación de prevención de riesgos laborales*, Informe 434/2004, disponible en: *https://www.aepd.es/es/documento/2004-0434.pdf*.

Agencia Española de Protección de Datos, 1999, *Naturaleza de los datos psicológicos a efectos de su tratamiento,* disponible en: *https://www.aepd.es/es/documento/1999-9908.pdf*.

Article 29 Working Party, 2017, *Guidelines on Data Protection Impact Assessment [DPIA] and determining whether processing is "likely to result in*

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

a high risk" for the purposes of Regulation 2016/679, disponible en: *http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.*

Article 29 Working Party, 2011a [Carta para Madame le Bail], 20 de abril, disponible en: *https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_en.pdf.*

30 Article 29 Working Party, 2011b, *Advice paper on special categories of data ("sensitive data")*, disponible en: *https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf.*

Comité Europeo de Protección de Datos, 2018, *Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b),* disponible en: *https://edpb.europa.eu/our-work-tools/our-documents/opinia-art-70/opinion-232018-commission-proposals-european-production_es.*

Conferencia Internacional de Comisionados de Protección de Datos y Privacidad, 2018, *Declaration on ethics and data protection in Artificial Intelligence*, Brussels, disponible en: *https://edps.europa.eu/sites/edp/files/publication/icdppc-40th_ai-declaration_adopted_en_0.pdf.*

C-101/01 (*Caso Bodil Lindqvist*), 2003, Tribunal de Justicia de la Unión Europea, disponible en: *http://curia.europa.eu/juris/liste.jsf?num=C-101/01.*

Federal Communications Commission, 2016, *Report and Order (FCC 16-148): In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* disponible en: *https://www.fcc.gov/document/fcc-releases-rules-protect-broadband-consumer-privacy.*

Information Commissionaire's Office, 2013, *Proposed new EU General Data Protection Regulation Article-by-article analysis paper,* disponible en: *https://ico.org.uk/media/about-the-ico/documents/1042564/ico-proposed-dp-regulation-analysis-paper-20130212.pdf.*

Information Commissionaire's Office, 2011, *The Information Commissioner's (United Kingdom) response to a* comprehensive *approach on personal data protection in the European Union. A Communication from the European Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on 4 November 2010.*

United States v. Jones, 2012, Supreme Court of the United States of America, 565 U.S. 400.

DOI: http://dx.doi.org/ 10.22201/iij.25940082e.2020.10.14658

2. *Marco jurídico internacional*

Autoridades de Protección de Datos y Privacidad, 2009, *Estándares Internacionales sobre Protección de Datos Personales y Privacidad* (Resolución de Madrid), disponible en: *https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf*.

Congreso Nacional de Chile, 1999, *Ley 19628 sobre Protección de la Vida Privada*, disponible en: *https://www.leychile.cl/Navegar?idNorma=141599&buscar=19628*.

Congreso de la República de Colombia, 2012, *Ley Estatutaria 1581*, por la cual se dictan disposiciones generales para la protección de datos personales, disponible en: *http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html*.

Council of Europe, 1981a, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, núm. 108, disponible en: *https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37*.

Council of Europe 1981b, *Explanatory Report to the Convention for the Protection of Individuals with* regard *to Automatic Processing of Personal Data*, disponible en: *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434*.

Organización para la Cooperación y el Desarrollo Económicos, 1980, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, disponible en: *http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm*.

Organización de las Naciones Unidas, 1990, Resolución 45/95, 14 de diciembre, *Principios rectores para la reglamentación de los ficheros computarizados de datos personales,* disponible en: *https://undocs.org/sp/A/RES/45/95*.

Reglamento General de Protección de Datos, 2016, Reglamento (UE) 2016/679, 27 de abril, disponible en: *https://www.boe.es/doue/2016/119/L00001-00088.pdf*.

Reglamento General de Protección de Datos, 1995, Directiva 95/46/CE, 24 de octubre, disponible en: *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML*.