Revista de la Facultad de Derecho de México
Tomo LXX, Número 278, Septiembre-Diciembre 2020
DOI: http://dx.doi.org/10.22201/fder.24488933e.2020.278-2.77065

La protección de los datos personales como derecho fundamental: su autonomía y vigencia propia en el ordenamiento jurídico estatal

Data protection as a fundamental right: its autonomy and its own validity in the State's legal system

Pascal Peña-Pérez[*]

Resumen: Prerrogativas del ordenamiento jurídico clásico, tales como el derecho al honor, intimidad o privacidad, entre otros, comenzaron a ser insuficientes ante la nueva realidad que representa el Internet y la interactividad digital. Consecuencia de ello, la protección de los datos personales surge como una prerrogativa con características propias y no dependiente de otros derechos de corte tradicional, reconocida en legislación especializada a nivel mundial y, algunos países como la República Dominicana, consagrada en su Constitución política.

Palabras clave: Datos personales; derechos fundamentales; tratamiento de datos; derechos tradicionales; derecho autónomo.

---

[*] Abogado. Doctor (Phd) en Derecho Internacional y Relaciones Internacionales por la Universidad Complutense de Madrid (UCM) y candidato a post doctorado en Derecho y Nuevas Tecnologías en el Mediterranea International Center for Human Rights Research (Reggio Calabria, Italia). Es docente en la República Dominicana en la Pontificia Universidad Católica Madre y Maestra (PUCMM) y la Universidad Iberoamericana (UNIBE). Es socio fundador en la firma ALIES PASCAL-Abogados, en la República Dominicana. Email: <pascalpena@yahoo.com>; Redes: <@PascalPenaP>. Fecha de recepción: 30/07/20. Fecha de aprobación: 15/10/20.

DOI: http://dx.doi.org/10.22201/fder.24488933e.2020.278-2.77065

Abstract: The prerogatives of the classical legal system, such as the right to honor, intimacy or privacy, among others, were beginning to be insufficient in the face of the new reality that the Internet and digital interaction currently represent. Consequently, the protection of personal data arises as a prerogative with its own characteristics and not dependent on other rights of a traditional nature, recognized in specialized legislation worldwide and, in some countries such as the Dominican Republic, enshrined in its Political Constitution.

Keywords: Personal data; fundamental rights; data processing; traditional rights; autonomous right.

I. Prolegómeno

La sociedad de la información ha fomentado una interactividad constante permitiendo más eficiencia en los procesos, la reducción de los costos asociados a diversas transacciones, la desaparición de las fronteras geográficas y, especialmente, se ha democratizado el acceso a la información y su control. A pesar de sus ventajas, también han surgido nuevos desafíos como resultado de que se ha colocado en manos de terceros el control y destino de los datos obtenidos a través de la web o cualquier otro medio de tratamiento de datos. Prerrogativas del ordenamiento jurídico clásico -vg. derecho al honor, intimidad o privacidad, secreto de las comunicaciones y correspondencia, inviolabilidad del domicilio entre otros-, comenzaron a ser insuficientes ante esta nueva realidad virtual.

Consecuencia de esto, algunos países han reconocido en su ordenamiento jurídico nuevos derechos relacionados a esta nueva realidad, a los cuales se les ha provisto obligaciones y mecanismos específicos de tutela: Uno de estos es la protección de datos personales, tema objeto de nuestro estudio. Para comprender su existencia y objeto, se debe conocer el origen y desarrollo de esta prerrogativa

II. La delimitación conceptual del derecho a la protección de datos

El derecho de protección de datos personales persigue pragmáticamente garantizar -y no solo conceptualmente obligar- que terceros se abstengan de toda intromisión en la esfera íntima (dimensión negativa), sino también un poder de disposición y de control sobre el uso y destino de estos datos (dimensión positiva). En este sentido, podemos definir que un *dato de carácter personal* es toda información concerniente a personas físicas identificadas o iden-

DOI: http://dx.doi.org/10.22201/fder.24488933e.2020.278-2.77065

tificables, que pueda servir para la confección de un perfil de ella. Como ejemplo de estas informaciones, se encuentran el nombre y los apellidos, la dirección, documento nacional de identidad (DNI o cédula), su fotografía, un video donde aparezca o una grabación de su voz, el número de su cuenta bancaria, ciertos datos familiares, información sobre cualquier tipo de actividad desarrollada en el ámbito de sus relaciones laborales, económicas o sociales, referencias ideológicas, raciales, étnicas, religiosas o de cualquier otra índole,[1] o datos de salud en poder de un hospital o médico.

Asimismo, son considerados datos personales las *cookies* (o galleta informática). En sí mismas, son inofensivas porciones de información que se almacenan localmente en un dispositivo para adaptar su contenido y ofrecerle uno más apropiado según sus hábitos de navegación. Estas cookies se pueden ver y eliminar fácilmente. Sin embargo, si las cookies se llevan un registro de la actividad previa del usuario, siendo capaces de identificar a un individuo a través de sus hábitos de navegación y preferencias del usuario,[2] se requerirá el consentimiento expreso e inequívoco del usuario para que su información sea tratada. Igualmente puede ser considerado como dato personal, la dirección de protocolo de internet (IP),

[1] España, Tribunal Constitucional, Sentencia núm. 292/2000 del 30 de noviembre de 2000.

[2] En este sentido, hay cookies donde no se requiere informar ni obtener el consentimiento previo del usuario, tales como las cookies de entrada (rastrean las acciones del usuario relativas al relleno de formularios en línea), las cookies de identificación del usuario (recuerdan tus claves de acceso a la web) y las cookies de sesión (relacionadas a la reproducción y difusión de contenido multimedia, por ejemplo.) Sin embargo, existen otros tipos de cookies que sí obligan a informar y obtener el consentimiento para su instalación y utilización, a saber: (i) las cookies de análisis: son aquellas relativas al seguimiento y análisis del comportamiento de los usuarios en los sitios web. Con ello, se elabora un perfil del usuario visitante; y, (ii) Cookies de publicidad comportamental: con el levantamiento de los datos revelados en sus hábitos de navegación, se personaliza la publicidad que se le muestra a cada usuario en la web.

cuya función es identificar un dispositivo con la capacidad de conectarse a internet -vg. computadora, tableta, celular, etc-. Algunos cuestionan su naturaleza de dato personal porque afirman que no se asocia un número al dispositivo de un usuario particular[3] y, por tanto, es difícil asociar dicha información a una persona debido a que sin una orden judicial los proveedores de servicios de Internet no entregan la identificación de las personas asociadas a esas IP (el nombre del usuario).

Consecuencia de lo anterior, podemos interpretar que la normativa dominicana considera el IP como un dato personal a partir del concepto de "secreto de las comunicaciones"[4], ya que impone a los prestadores de servicios de telecomunicaciones una obligación de secreto que, en palabras de Tribunal Constitucional, "abarca no solamente el contenido o carácter privado de la misma, sino que además incluye todo el proceso mismo en que se da la comunicación, entre ellos la identidad de los interlocutores, el momento,

[3] En efecto, la dirección IP es un número único asignado a cada equipo conectado al Internet y que, en general, cambia cada vez que se conecta a éste (IP dinámico). Sin embargo, con algunas conexiones de banda ancha la dirección IP es estática porque se le asigna una dirección IP específica que se asocia a un dispositivo particular. Por supuesto, las direcciones IP no identifican la identidad de la persona, pero puede identificar al proveedor de servicios de Internet que asignó esa IP a cada dispositivo y este, a su vez, puede describir los datos de contacto que tienen registrados de la persona física o jurídica a la que le fue asignado esa IP.

[4] República Dominicana, Consejo Directivo del INDOTEL, Reglamento de Derechos y Deberes de los Usuarios y las Prestadoras, dictada mediante Resolución núm. 062-17, art. 11; República Dominicana, Reglamento General del Servicio Telefónico, dictado mediante Resolución núm. 110- 12 del Consejo Directivo y modificado mediante las resoluciones núm. 003-13 y núm. 062-17, arts. 28 y 29; Reglamento para la Solución de Controversias, dictada mediante Resolución núm. 013-17 del Consejo Directivo del INDOTEL, art. 5.10 y 5.11. Asimismo, ver el art. 44 inciso 1 de la Resolución núm. 055-06, dictada por el Consejo Directivo del INDOTEL.

DOI: http://dx.doi.org/10.22201/fder.24488933e.2020.278-2.77065

DOI: http://dx.doi.org/10.22201/fder.24488933e.2020.278-2.77065

duración y destino de la misma."[5] Este mismo punto de vista ha sido asumido por países como España,[6] Costa Rica[7] y El Salvador[8], pudiendo considerarse que este secreto subsiste tras la finalización del proceso de comunicación y, en cuya virtud, queda prohibida toda información sobre el contenido y las circunstancias de las comunicaciones del usuario. Sea cual fuere la perspectiva, se debe valorar en que siempre que la dirección IP permita identificar a una persona física, deberá estimarse que estaremos ante un dato personal. Con ello, el usuario tiene la posibilidad de oponerse a que determinados datos personales sean utilizados para fines distintos a aquellos que motivaron su obtención.[9] De lo anterior se infiere que, si bien se encuentra vinculado a otros derechos de corte tradicional -como el derecho al honor, intimidad, secreto de las comunicaciones y correspondencia, inviolabilidad del domicilio entre

[5] República Dominicana, Tribunal Constitucional, Sentencia núm. TC/0200/13 del 7 de noviembre de 2013.

[6] En España, el art. 41 de la Ley núm. 9/2014 establece que "los operadores, también conocidos como las prestadoras de servicios públicos de telecomunicaciones, deberán garantizar la protección de los datos de carácter personal."

[7] En Costa Rica el art. 42 de la Ley núm. 8642 General de Telecomunicaciones del 04 de junio de 2008 establece que los operadores tendrán que adoptar medidas para garantizar la seguridad en sus redes y además deben garantizar el secreto de las comunicaciones.

[8] En El Salvador el art. 29, literal b, de la Ley General de Telecomunicaciones (Decreto Ley núm.142 del 6 de noviembre de 1997, ordena como derecho de los usuarios el secreto de sus comunicaciones y la confidencialidad de sus datos personales no públicos, y tiene en cuenta lo mencionado en el título V-bis, Capítulo Único de la presente ley. En ese orden, el art. 42-H de la mencionada ley prohíbe a las autoridades a interferir o intervenir comunicaciones telefónicas con respeto a lo dispuesto por el art. 24 de la Constitución. Asimismo, este artículo reconoce la inviolabilidad de la correspondencia.

[9] Cfr. España, Tribunal Constitucional, Sentencia núm. 11/1998 y Sentencia núm. 94/1998, fundamento jurídico 5.

otros- la protección de datos personales debe ser vista en la República Dominicana como un derecho fundamental autónomo.[10]

III. Titularidad del derecho de protección de datos personales

Oportuna es la ocasión para determinar si una persona moral o jurídica es también titular de datos personales. Como punto de partida se debe señalar que las personas jurídicas son titulares de ciertos derechos fundamentales[11] que, a su vez, le permite hacer uso de las garantías procesales reconocidas en la Constitución.[12] En efecto, como hemos afirmado, las personas jurídicas "sí son titulares de ciertos derechos fundamentales de naturaleza dual que, en tanto y en cuanto sirvan para proteger su propia existencia e identidad, el libre desarrollo de su actividad o que sean necesarios y complementarios para la consecución de los fines para los que han sido creadas, pueden ser ejercidos tanto por individuos como por agrupaciones."[13] Como ejemplos de estos derechos, podemos citar la libertad de empresa, el derecho de propiedad, el debido proceso, la intimidad y el honor, la libertad de expresión e información, la libertad de asociación, entre otros.[14]

---

10 Tal como lo hicieron hace décadas el Tribunal Constitucional alemán y el Tribunal Constitucional español. Vid. España, Tribunal Constitucional, Sentencia núm. 254/1993 del 20 de julio de 1993; Sentencia núm. 11/1998 del 13 de enero de 1998 y Sentencia núm. 94/1998 del 4 de mayo de 1998.

11 República Dominicana, Tribunal Constitucional, Sentencia núm. TC/0027/12 del 5 de julio de 2012, párr. 9.12; Cfr. Sentencia núm. TC/0563/15 del 4 de diciembre de 2015, párr. 10.10.4.

12 República Dominicana, Tribunal Constitucional, Sentencia núm. TC/0404/16 del 9 de septiembre de 2016., párr. o.

13 Cfr. Peña Pérez, Pascal, "La definición de la indefinición del derecho al honor", República Dominicana, *Gaceta Judicial,* noviembre de 2007.

14 Cfr. República Dominicana, Tribunal Constitucional, Sentencia núm. TC/0404/16 del 9 de septiembre de 2016, párr. e.

DOI: http://dx.doi.org/10.22201/fder.24488933e.2020.278-2.77065

Aclarado lo anterior corresponde ahora determinar si, entre los derechos fundamentales de las personas jurídicas, se encuentra la protección de sus datos personales. En el caso de la República Dominicana, la Constitución política no discrimina entre personas físicas y jurídicas cuando reconoce el derecho a la protección de datos pero, en su normativa especial, específicamente en el sector de las telecomunicaciones, puntualiza que "[l]os datos relativos a personas jurídicas no serán considerados Datos de Carácter Personal.[15] Este tema tiene especial relevancia puesto que es incuestionable que cualquier sociedad comercial, asociación o, en general, toda persona jurídica, puede sufrir intromisiones arbitrarias a informaciones de índole tecnológico, científico, económico, comercial que, de revelarse "(…) pudiera anular o menoscabar su libre y buen desarrollo."[16] Asimismo, este acceso y posible uso no autorizado de información confidencial o privilegiada, podría configurar una competencia desleal en el marco del Derecho de la competencia,[17] ya que menoscabaría de forma ilegítica la capacidad competitiva.

Sobre estos datos de naturaleza especialmente sensible para las empresas, la Suprema Corte de Justicia de México ha afirma-

---

15 República Dominicana, Resolución núm. 055-06 del Consejo Directivo del Instituto Dominicano de las Telecomunicaciones (INDOTEL), 23 de marzo de 2006. "Los datos relativos a personas jurídicas no serán considerados Datos de Carácter Personal, sin perjuicio de aquellos datos relativos a personas naturales que se encuentren vinculadas a dichas personas jurídicas que, si podrán ser considerados como Datos de Carácter Personal, comprendiendo, entre otros, los datos de sus representantes, apoderados o trabajadores".

16 México, Suprema Corte de Justicia de la Nación, Pleno, Tesis: 2005522. P. II/2014 (10a.), *Gaceta del Semanario Judicial de la Federación*, libro 3, t I, febrero de 2014, p. 274.

17 República Dominicana, Ley General de Defensa de la Competencia, núm. 42-08, 25 de enero de 2008, art. 10, d); Cfr. Ley General de Telecomunicaciones, núm. 153-98, art. 1; Cfr. Ley sobre Propiedad Industrial, núm. 20-00, art. 176

do que "los bienes protegidos por el derecho a la privacidad y de protección de datos de las personas morales, comprenden aquellos documentos e información que les son inherentes, que deben permanecer ajenos al conocimiento de terceros (…), la información entregada a las autoridades por parte de las personas morales, será confidencial cuando tenga el carácter de privada por contener datos que pudieran equipararse a los personales, o bien, reservada temporalmente, si se actualiza alguno de los supuestos previstos legalmente."[18] Por tanto, se puede afirmar que las personas jurídicas son titulares del derecho a la protección de datos, más no a la protección de datos personales, puesto que es un derecho de naturaleza personalísima y del cual solo gozan las personas físicas. Sin embargo, tal como lo ha expresado el Tribunal Constitucional de la República Dominicana, existe un derecho a la privacidad de la empresa o lo que ha desarrollado la teoría española como un derecho a la fidelidad empresarial, equiparable por su naturaleza al derecho de protección de datos personales, "que firman las partes para no divulgar cuestiones propias de una empresa."[19] Estas informaciones de carácter confidencial cuya titularidad poseen las personas jurídicas son, como explicamos, equiparables a la salvaguardia dada a las personas físicas en tanto que el tratamiento que

[18] Cfr. México, Suprema Corte de Justicia, Pleno, Materia: Constitucional, Gaceta del Semanario Judicial de la Federación Libro 3, febrero de 2014, Tomo I, Tesis: P.II/2014 (10a.), p. 274. En la República Dominicana, podemos mencionar entre las informaciones que no pueden revelarse aquellas declaradas como "confidenciales" por los entes del Estado en materias específicas ante la entrega voluntaria o solicitada por el depositante. Ejemplo de ello son las informaciones depositadas ante la Comisión de Defensa Comercial en virtud de la Ley núm. 1-02 o la Comisión Nacional de Defensa de la Competencia en virtud de la Ley núm. 42-08 en el marco de una investigación; o las informaciones entregadas por las prestadoras de servicios de telecomunicaciones al INDOTEL.

[19] República Dominicana, Tribunal Constitucional, Sentencia núm. TC/0027/12 del 5 de julio de 2012, párr. 9.12.

DOI: http://dx.doi.org/10.22201/fder.24488933e.2020.278-2.77065

se le dé a su información, debe tener su consentimiento expreso e inequívoco. En caso de violación a sus derechos, la persona jurídica podrá ejercer las acciones administrativas y judiciales que considere pertinente.

IV. El origen de la protección de datos personales como derecho fundamental autónomo

El nivel de desarrollo económico, social y cultural de cada país condiciona el alcance de protección de los derechos fundamentales de los cuales es titular. A mayor desarrollo, mayor es el nivel de resguardo. En este sentido, al estudiar la experiencia comparada, es claro notar que Europa posee un robusto sistema jurídico que cuenta con normativa comunitaria y nacional especializada en el tema. Tradicionalmente se reconocen y protegen en el ámbito constitucional de los Estados derechos como el de la privacidad, intimidad, inviolabilidad de domicilio y secreto de las comunicaciones, entre otros. Con el auge de las nuevas tecnologías, diversos países incorporaron en su legislación la protección de datos personales y el *habeas data* para su tutela. Tal es el caso de Portugal, quien incluyó en su Constitución el término en el año 1976[20] y en América Latina países como Perú y Venezuela limitan el uso de la informática si puede afectar derechos como el honor, vida privada,

[20] Portugal, Constitución política, 1976, art. 35.1: "Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización". Este texto luego fue modificado para adaptarlo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, la cual fue a su vez derogada en el 2016 por el Reglamento General de Protección de Datos (RGPD). Igualmente, otros países como España, incluye en el artículo 18.4 de su Constitución (1978) referencia a los limites "del uso de la informática para garantizar el honor y la intimidad"

intimidad, entre otros. Otros países de la región, como Argentina, Brasil, Colombia, Ecuador, Guatemala, Nicaragua y la República Dominicana, en su normativa constitucional reconocen el derecho a toda persona de conocer los datos que sobre ella reposen en bancos de datos, sea de naturaleza pública o privada, tutelándose además a través de la acción del *habeas data*.[21] Sin embargo, pese

[21] Argentina establece en el art. 43. 3 de su Constitución el *habeas data*, así como también posee una la Ley núm. 25.326 de protección de datos personales, debidamente reglamentada en el 2001, texto normativo que es una de las primeras leyes de protección de datos en América Latina, con una autoridad específica de control. En 2018, se propuso un proyecto de ley para modificar el referido texto con el fin de ajustarla con el Reglamento General de Protección de Datos (RGPD); en Bolivia, se carece de una ley específica para regular la protección de datos. Sin embargo, el art. 21. 2 de la Constitución reconoce el "derecho a privacidad, intimidad, honra, propia imagen y dignidad" y los arts. 130 y 131 de dicho texto reconoce el *habeas data,* además tiene una ley de delitos informáticos que cubre ciertos aspectos relacionados con la privacidad de las personas; en Brasil fue promulgada en el año 2018 su Ley General de Protección de Datos, alineada a las disposiciones de RGPD. Además de esto, su Constitución regula el *habeas data* y la protección de la intimidad, vida privada y secreto de las comunicaciones. Asimismo, poseen varias leyes en sectores como bancos de datos, consumo, secreto bancario, entre otros; Chile posee en el art. 19. 4 de su Constitución la protección a la vida privada y pública, así como el derecho a la honra. De igual forma, tiene la Ley núm.19628 sobre protección de la vida privada del año 1999 (modificada en 2002), la cual es una ley general y no contempla una autoridad de control o única encargada de garantizar la protección de datos. Al igual que Brasil, posee numerosas normativas sectoriales, tales como, en lo laboral, información financiera o de salud, entre otras. Recientemente ha buscado reformar la Ley núm.19628 para ajustar sus disposiciones al RGPD;Colombia reconoce en el art. 15 de su Constitución la protección de la intimidad. Posee además la Ley n.º 1581 de protección de datos personales y la Ley núm.1266 sobre *habeas data* y regula el manejo de información contenida en base de datos personales. En la actualidad Colombia debate un proyecto legislativo que pretende dotar a la Ley n.º 1581, relativa a la privacidad de datos,

DOI: http://dx.doi.org/10.22201/fder.24488933e.2020.278-2.77065

con un alcance internacional similar al del RGPD; Costa Rica reconoce en los arts. 23 y 24 de su Constitución la protección del domicilio, así como la intimidad y secreto de las comunicaciones, respectivamente. Asimismo, posee la Ley núm.8968 del año 2011, sobre protección de la persona frente al tratamiento de sus datos personales, la cual establece como autoridad de control a la Agencia de Protección de Datos de los Habitantes (Prodhab), órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz; Ecuador posee en los art. 23. 8 y 23. 21 de la Constitución sobre la intimidad personal y la prohibición de uso de la información personal, respectivamente. El art. 94 de ese mismo texto recoge el *habeas data*. Asimismo, posee leyes sectoriales que se refieren al tema, como la Ley de Comercio Electrónico y la Ley de Estadísticas y Censos; México posee en el art. 16 de su Constitución la protección al derecho de privacidad. Además, posee en su Ley Federal de Transparencia y Acceso a la Información Pública de 2002 un título dedicado a la protección de datos personales. Al igual que los demás países descrito, México posee numerosas normativas sectoriales, tales como, en materia de salud, en sociedades de información crediticia, entre otras. En el año 2010, México promulgó la Ley Federal Mexicana de Protección de Datos Personales en Posesión de los Particulares, la cual rige el tratamiento de datos personales. Asimismo, tiene una autoridad de control con autonomía constitucional; Nicaragua posee en el art. 26 de su Constitución la protección a la vida privada e inviolabilidad de la correspondencia. De igual forma, posee en su marco normativo la Ley núm.787 de protección de datos personales y la autoridad de control es la Dirección de Protección de Datos Personales, adscrita al Ministerio de Hacienda y Crédito Público; en Panamá no existe disposición constitucional específica, excepto la de inviolabilidad de correspondencia, ni tampoco existe una norma general. Sin embargo, cuenta con leyes sectoriales sobre transparencia en la gestión pública -Ley núm.6 de 2002- o la de información crediticia -Ley núm.25 del 23 de mayo de 2002-; Paraguay reconoce la inviolabilidad de la intimidad personal y vida privada en su art. 33 y, en su art. 135, recoge el *habeas data*. Asimismo, posee la Ley núm.1682 del 16 de enero de 2001 (modificada en 2002); en Perú existe la Ley núm.29733 de protección de datos personales del año 2011, esta regula la materia y establece una autoridad nacional de protección de datos personales; en Uruguay la Constitución recoge en su arts. 7, 11 y 28 la protección al honor, la inviolabilidad del hogar y la

a las recomendaciones y directrices elaboradas por organizaciones internacionales,[22] América Latina tienen un régimen fragmentado, con normas concebidas acorde con una realidad territorial.

Salvo contadas excepciones, el nivel de madurez en la implementación de marcos normativos y regulatorios en los países de la región refleja que la República Dominicana y la mayoría de los países de América Latina carecen de los mecanismos suficientes a los estándares exigidos por regímenes jurídicos más desarrollados -como el de la Unión Europa y el RGPD-. Es paradójico que, pese a la República Dominicana tener plasmado la protección de datos personales en la Constitución desde el año 2010 -lo que podría parecer un avance frente a otros países de la región latinoamericana-, países como Argentina y Uruguay han asumido en la práctica un ejercicio respetuoso con cuerpos legales sectoriales. [23]

---

inviolabilidad de la correspondencia, respectivamente. Asimismo, posee la Ley núm.18331 de 2008 sobre protección de datos personales y *habeas data*, la cual establece el órgano de control que es la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). De igual forma, en su sistema jurídico existen diversas normas sectoriales, como es la Ley núm.16736 sobre acceso frente a la administración, el Código de la Niñez y Adolescencia (2004), entre otras.

[22] Entre ellas, podemos mencionar a la Organización de Naciones Unidas (ONU), Foro de Cooperación Económica Asia Pacifico (APEC), Organización para la Cooperación y el Desarrollo Económicos (OCDE); y regionales como la Red Iberoamericana de Protección de Datos. Véase, por ejemplo, Red Iberoamericana de Protección de Datos, *Directrices para la armonización de la protección de datos en la comunidad iberoamericana*, disponible en: <http://www.redipd.es/actividades/encuentros/V/common/9_nov/Directrices_de_armonizacion.pdf>.

[23] El RGPD faculta a las autoridades de la Unión Europea para investigar y evaluar si un país, sector o una organización internacional garantiza un nivel adecuado de protección a los datos personales de los. Como resultado de ello, en la región latinoamericana, la Comisión Europea solo reconoce actualmen-

DOI: http://dx.doi.org/10.22201/fder.24488933e.2020.278-2.77065

Sin embargo, antes de plasmarse este derecho en la Carta Magna, el término "datos" o "datos personales" ya había sido reconocido en el ordenamiento jurídico doméstico dentro de la Ley General de Telecomunicaciones, núm. 153-98.[24] Es en el año 1998, por tanto, la primera vez que el sistema normativo de la República Dominicana recoge la figura de los datos personales. Cuatro años después, se precisa a través de otro texto legal el alcance del término al indicar que es "[l]a información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares."[25] La concreta definición de la figura de "datos de carácter personal", se

---

te a Argentina y Uruguay como países que garantizan un nivel de protección adecuado.

[24] El art. 5 indica que "[l]as comunicaciones y las informaciones y *datos emitidos por medio de servicios de telecomunicaciones son secretos e inviolables.*" [resaltados nuestros] Vid. República Dominicana, Ley General de Telecomunicaciones, núm. 153-98, 27 de mayo de 1998.

[25] República Dominicana, Ley sobre Comercio Electrónico, Documentos y Firmas Digitales, núm. 126-02. En ella, el art. 2, literal c lo definió de la manera siguiente: "Mensajes de datos: La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el telex o el telefax". Vid. Ley sobre el Comercio Electrónico, Documentos y Firmas Digitales, No. 126-02. Asimismo, el ordenamiento jurídico de la República Dominicana también se compone por la Ley sobre Libre Acceso a la Información Pública, núm. 200-04, la cual, conceptualmente inspirada por la normativa mejicana de la época, (Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental Publicada en el Diario Oficial de la Federación el 11 de junio de 2002, derogada por la Ley Federal de Transparencia y Acceso a la Información Pública, 9 de mayo de 2016) incorpora la figura de protección de datos personales al derecho interno como límite al acceso a la información considerada de acceso público, y su entrega solo es posible cuando cuenta con el consentimiento expreso e inequívoco del titular. Vid. República Dominicana, Ley General de Libre Acceso a la Información Pública, núm. 200-04, 28 de julio del 2004, arts. 18-20.

recoge por primera vez en el país en año 2006 cuando se indica en una norma también del sector de las telecomunicaciones, que el término engloba "cualquier información concerniente a personas naturales identificadas o identificables."[26] Esta definición, vale resaltar, parece haber sido extraída de la derogada Directiva 95/46/CE del Parlamento Europeo y del Consejo y que subsiste en el Reglamento General de Protección de Datos de la Unión Europea (en lo adelante, "RGPD")*.*[27]

Sin embargo, es en el año 2010 cuando en la República Dominicana el derecho de protección de datos personales es reivindicado como una prerrogativa autónoma en el país. En efecto, el 26 de enero de 2010 fue promulgada la nueva Constitución política del país, estableciendo en su art. 44.2 lo siguiente:

"2) Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se

[26] República Dominicana, Consejo Directivo del INDOTEL, Resolución núm.055-06 del 23 de marzo de 2006 que aprueba la norma complementaria de la Ley núm. 126-02 sobre Protección de Datos de Carácter Personal por los Sujetos Regulados, art. 2, literal i. Vale resaltar que dicha definición se encuentra acorde, con lo expuesto en el Convenio 108 del Consejo Europeo, que define datos personales como *cualquier información relativa a una persona física identificada o identificable («persona concernida»)* [Resaltados nuestros]. Cfr. Unión Europea, Convenio 108 del Consejo de Europa del 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, art. 2 literal a). Luego con la Ley sobre Crímenes y Delitos de Alta Tecnología, núm. 53-07, plasmó nuevamente el término *dato* -aunque omite el término "de carácter personal"- y, al definirlo, prosiguió la línea conceptual de la Ley de Comercio Electrónico. En este sentido, la Ley núm. 53-07 estableció que *dato* "es toda información que se transmite, guarda, graba, procesa, copia o almacena en un sistema de información de cualquiera naturaleza o en cualquiera de sus componentes." República Dominicana, Ley sobre Crímenes y Delitos de Alta Tecnología, núm.53-07, 23 de abril de 2007.

[27] Unión Europea, RGPD, Art. 4.1

DOI: http://dx.doi.org/10.22201/fder.24488933e.2020.278-2.77065

haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos;" [28]

Sin embargo, como la figura de protección de datos conlleva la posibilidad de solicitar la modificación, exclusión o actualización de alguna información, diferenciado de estos otros derechos que están destinados al resguardo de la personalidad, se crea el *habeas data* como tutela judicial.[29] Por ello, en el año 2013, fue promulgada en el país la Ley Orgánica de Protección de Datos Personales, núm. 172-13 (en lo adelante, la LOPDP-RD),[30] la cual afirma que "datos de carácter personal" es "[c]ualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"[31] y se establece el procedimiento judicial aplicable para ejercer el *habeas data* como garantía de tutela de esta prerrogativa.

---

[28] Cfr. CRD, art. 44 e.

[29] Otros sectores promovían la modificación de la Ley núm. 288-05 sobre información crediticia. Consecuencia de esta coyuntura, el Poder Legislativo promulgó en el año 2013 la citada LOPD-RD, donde su alcance fue destinado exclusivamente al sector monetario y financiero, y el órgano de control es la Superintendencia de Bancos, organismo del Estado dominicano concebido exclusivamente para supervisar a las entidades de intermediación financiera y el cumplimiento de la normativa de dicho sector por parte de ellas, República Dominicana, Ley Monetaria y Financiera, núm. 183–02, 21 de noviembre de 2002, art. 19.

[30] Esta ley deroga la Ley núm. 288-05 que regulaba las Sociedades de Información Crediticia y de Protección al Titular de la Información, la cual se enfocaba en regular la protección de los datos asentados en bases de datos crediticias.

[31] Cfr. República Dominicana, LOPDR-RD, art. 6.9.

Contrario al mencionado régimen fragmentado que muestra la República Dominicana y otros países de Latinoamérica en materia de protección de datos, Europa posee un sistema organizado que le permite alcanzar sus objetivos eficientemente, incluso fuera del territorio de la Unión Europea. En efecto, el citado RGDP (2016) fue diseñado para proteger los datos personales de usuarios europeos, cualquiera que sea la jurisdicción en donde se procesen. Para cumplir con su objetivo, esta norma a las personas o empresas ubicadas en la Unión Europea que traten datos personales -v.g. página web que ofrece bienes o servicios a residentes europeos-, así como también a las empresas ubicadas en otros países que traten información personal de ciudadanos europeos, -v.g. rastreo de cookies, ip-.[32] Consecuencia de lo anterior, si una empresa dominicana, mejicana o de cualquier otro país tiene una tienda online, que despacha pedidos para Europa, o una página web que brinda cursos virtuales -pagos o gratuitos- y residentes europeos acceden a dichos servicios, esta debe someterse a las obligaciones establecidas por el RGPD (2016).

Como resultado del importante papel que juega la Unión Europea para los mercados e industrias de Latinoamérica, varios países han reformado su legislación.[33] A finales de 2019, en la República Dominicana se conformó una comisión multidisciplinar[34] para redactar, con el apoyo del Consejo de Europa, un proyecto de

[32] Unión Europea, RGPD, art. 4.

[33] Brasil, por ejemplo, en el año 2018 promulgó una ley de protección de datos alineada al RGPD, mientras que países como Argentina, Chile y México han tomado medidas para aumentar los niveles de protección.

[34] El Ministerio de la Presidencia conformó en el año 2019 un grupo multidisciplinar, del cual el autor de este trabajo fue parte. En el mismo se encontraban miembros del Instituto Dominicano de las Telecomunicaciones (INDOTEL), representantes de la Policía Nacional, representantes de la Procuraduría General de la República, representantes de la Dirección General de Ética e Integridad Gubernamental (DIGEIG), representantes del Poder Judicial, representantes de la sociedad civil, entre otros. Del Consejo de Europa,

DOI: http://dx.doi.org/10.22201/fder.24488933e.2020.278-2.77065

Ley General de Protección de Datos cuyo borrador aún no ha sido presentado al Congreso Nacional. Se debe resaltar, sin embargo, que está claramente influenciado por el RGPD (2016) y por la ley española de protección de datos en los aspectos aplicables.

V. Derechos tradicionales que han evolucionado en el espacio digital

El goce y ejercicio de los derechos humanos en la era digital presenta importantes desafíos desde el ámbito práctico. De manera particular, cuando fueron concebidos y posteriormente reconocidos ciertos derechos -englobados hoy en la primera generación-, la virtualidad no era ni siquiera una idea. El reto de los ordenamientos jurídicos del mundo consistió en que, previo al surgimiento de nuevos derechos nacidos de esta nueva realidad, lograr que algunas prerrogativas clásicas mantuvieran su vigencia y lograran cierta efectividad. Entre ellas, podemos mencionar los derechos a la propia imagen (i), intimidad personal y familiar (ii), derecho al honor (iii); y, *Libertad de expresión y acceso a información (iv),* los cuales abordaremos a continuación, pero interpretados desde la virtualidad.

A) Derecho a la propia imagen

Las personas, físicas y jurídicas, tienen el derecho de captar, reproducir y publicar su propia imagen, así como requerir -o impedir- su reproducción de sin su autorización.[35] Si estudiamos el tema desde la óptica de las nuevas tecnologías, cuando se accede

asistieron al país especialistas internacionales para colaborar con la elaboración de texto.

[35] Ver República Dominicana, CRD, art. 44; Cfr. Peña Peña, Pascal, "El comercio de la imagen", *Listín Diario*, 1 de noviembre de 2007, disponible en: <https://listindiario.com/puntos-de-vista/2007/11/01/34968/el-comercio-de-la-imagen>.

a una plataforma digital, el usuario cede parte de sus derechos a los propietarios de esta cuando cuelga contenido en ella -vg. fotos, videos, mensajes, entre otros- puesto que podrían ser compartidos por terceros. Por igual, cuando una persona decide usar, grabar o compartir imágenes, videos o hasta capturas de conversaciones de whatsapp, esto será considerado un dato personal por cuanto se trata de información capaz de ser asociada a una persona e identificarla. [36]

B) Derecho a la intimidad o privacidad

El derecho a la intimidad o privacidad garantiza que no exista una divulgación no consentida de ciertos hechos relativos al círculo íntimo, personal y familiar de una persona o su familia y que, lógicamente, no haya sido publicada antes por el autor.[37] El derecho a la protección de datos personales se deriva de esta noción de intimidad o privacidad en tanto que supone el reconocimiento de un derecho a controlar el acceso a las informaciones que le conciernen a cada persona, así como su utilización y destino. Sin embargo, su ámbito de aplicación es más amplio ya que alcanza a todo tipo de datos, sean íntimos o no. De esta forma, se trata de preservar el pleno ejercicio de sus derechos y que la recopilación y tratamiento de los datos de la persona no propicie comportamientos discriminatorios o creación de perfiles. Es, en este aspecto, que entendemos útil traer a colación el derecho a la autodeterminación informativa,

---

[36] Colombia, Superintendencia de Industria y Comercio (SIC), Delegatura para la Protección de Datos Personales. Mediante concepto num. 33980, 2 de abril de 2013.

[37] Asamblea General de las Naciones Unidas, Declaración Universal de Derechos Humanos, Resolución 217 A (III) del 10 de diciembre de 1948, art. 12; Organización de los Estados Americanos, Convención Americana sobre Derechos Humanos (Pacto de San José del 22 de noviembre de 1969) del 11 de febrero de 1978; Pacto Internacional de Derechos Civiles y Políticos en sus arts. 14 y 17.

DOI: http://dx.doi.org/10.22201/fder.24488933e.2020.278-2.77065

ya que también ha adquirido autonomía y se concreta en la acción de *habeas data*. En la actualidad, sin embargo, este derecho a la autodeterminación informativa ha adquirido tal preponderancia que tiene especiales implicaciones en el entorno digital, tema que abordaremos en la segunda parte de esta investigación.

C) Derecho al honor

El honor es un concepto carente de *una definición incontrovertible y permanente*, pero se puede afirmar que este derecho está íntimamente relacionado con el prestigio social en tanto que su objetivo es proteger el buen nombre, la buena imagen pública y la buena reputación de las personas físicas o jurídicas.

El entorno virtual y la facilidad que todos tenemos en generar y publicar contenidos -a veces de forma anónima- y masificarse su transmisión y retransmisión a través de internet, es un alto riesgo para este derecho. Sobre esto, si bien existe la libertad de expresarse, no se puede ser ofensivo o procurar transgredir el derecho al honor de una persona. Asimismo, una cesión no consentida de datos personales puede configurar una violación al derecho de protección de datos personales y al derecho al honor cuando los datos eran falsos, estaban incompletos o no estaban actualizados y, por tanto, no cumplían el requisito de veracidad, afectando negativamente a la reputación del afectado. Por ello, el ejercicio de la libertad de expresión e información estará condicionado a respetar el derecho al honor.[38]

D) Libertad de expresión y acceso a información

La libertad de información y el acceso a la información son prerrogativas fundamentales en un Estado democrático. Su ejercicio,

[38] República Dominicana, Constitución, "Art. 49, Párrafo. - El disfrute de estas libertades se ejercerá respetando el derecho al honor, a la intimidad, así como a la dignidad y la moral de las personas, en especial la protección de la juventud y de la infancia, de conformidad con la ley y el orden público."

como el de ningún otro derecho, no es absoluto, debiendo existir un balance entre el legítimo interés que tiene cualquier usuario de buscar información y el derecho que tiene cualquier persona en oponerse a que sus datos personales aparezcan en internet o que determinada información no aparezca vinculada a su nombre. La publicación original que aparece en una página web no será, por tanto, la que genere el riesgo de violación a la protección de datos, sino que partiendo de los criterios dados por la sentencia Google (2014) [39] del Tribunal de la Unión Europea (TUE), una vez realizado el tratamiento de información por el buscador -Google, Yahoo!, entre otros-, se generan informaciones diversas que, asociadas entre ellas, introduce un impacto adicional a la publicación original. Consecuencia de ello, el ordenamiento jurídico debe crear una protección especial que mitigue la injerencia que representa el libre acceso y difusión de esta información personal a través un buscador.[40]

En resumen, para que no exista violación al derecho de protección de datos personales como resultado del legítimo derecho a la *libertad de expresión y acceso a información*, estos datos que se encuentra públicamente en la web podrán mantenerse asociados al titular siempre que esta información tenga naturaleza pública y sea de tal relevancia que sea noticiable. Este es el caso, por ejemplo, de publicaciones oficiales -vg. una sentencia judicial publicada en la página web del tribunal o en un boletín oficial-. Sobre el tema, el Tribunal Constitucional español ha establecido que para determinar el equilibrio entre estos derechos se deberá valorar la pertinencia de mantener esa información accesible al público (si la noticia es antigua y, por tanto, carece de efectos en la actualidad), si las personas que aparecen en ella no son personas públicas y si los datos que se revelan vulneran el derecho al honor y a la intimi-

[39] Tribunal de la Unión Europea (TUE), Google *Spain*, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, asunto C131/12 del 13 de mayo de 2014.

[40] *Ibidem*, párr. 38 y 80.

DOI: http://dx.doi.org/10.22201/fder.24488933e.2020.278-2.77065

dad con respecto al interés público de obtener esa información.[41] Por el contrario, cuando la información no cumple con estas dos condiciones, la solución será desindexar los datos que permiten identificar al titular de los datos personales en los motores de búsqueda de Internet.

VI. Reflexiones finales

El Internet y la virtualidad generó cambios profundos en los ordenamientos jurídicos de los países. Derechos como la propia imagen, a la intimidad o privacidad, al honor, libertad de expresión y acceso a información, son todavía útiles para proteger algunas de los conflictos suscitados en la interactividad. Sin embargo, estas prerrogativas que fueron concebidas para amparar los bienes jurídicos más básicas del ser humano dejaron de ser eficientes y suficientes ante esta nueva sociedad de la información. Como resultado de esto, surgió el derecho a la protección de datos personales, configurado como un derecho autónomo de exclusivo goce y ejercicio para las personas físicas, plasmado en leyes sectoriales en algunos países y, en la República Dominicana, en su Constitución política. Asimismo, esta virtualidad ha motivado el desarrollo de nuevas prerrogativas que acompañan la efectiva implementación de la protección de datos. Importante a resaltar es que el derecho a la protección de datos es muestra de la continua evolución de los ordenamientos jurídicos, a partir de las necesidades que surgen en la sociedad por el uso de las tecnologías y el tratamiento de datos personales.

[41] Ver por ejemplo, la sentencia dictada por el Tribunal Constitucional de España, donde ordenó a un periódico eliminar los datos de dos personas condenadas en los años 80. Disponible en: < https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2018_060/2016-2096STC.pdf>