Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

ANUARIO DE DERECHO CONSTITUCIONAL LATINOAMERICANO
AÑO XXVI, BOGOTÁ, 2020, PP. 697-722, ISSN 2346-0849

Carlos Ramón Salcedo Camacho* **(República Dominicana)**

Desafíos de la era digital en una sociedad hiperconectada: protección efectiva de los derechos fundamentales en la República Dominicana

RESUMEN

Los avances tecnológicos están transformando la realidad actual. La información se desplaza rápidamente. La conexión no detiene su crecimiento y los datos se convierten en activos de gran valor. Esta situación plantea desafíos en el ámbito jurídico, debido a que diversos derechos fundamentales son expuestos a nuevas situaciones que obligan a la transformación del derecho para proporcionar una protección adecuada, en la que los tribunales deben jugar un rol esencial.

Palabras clave: hiperconectividad; derechos fundamentales; proactividad jurídica.

Challenges of the digital age in a hyperconnected society: effective protection of fundamental rights in the Dominican Republic

ABSTRACT

Technological advances are transforming current reality. Information moves quickly. Connections do not stop growing, and data are converted into assets of great value. This situation poses challenges in the legal field, given that various fundamental rights are exposed to new situations that require the transformation of the law in order to provide adequate protection, in which the courts must play an essential role.

Keywords: Hyperconnectivity; fundamental rights; legal proactivity.

* Abogado, especialista en derecho constitucional, derechos fundamentales, libertades públicas, argumentación jurídica, derecho societario y comercial, legislación económica y empresarial, y derecho del trabajo y seguridad social. Autor y coautor de varias obras. Dirige la firma de abogados Salcedo & Astacio. carlos30salcedo@gmail.com. https://orcid.org/0000-0002-4222-5246.

VOLVER A TABLA DE CONTENIDO

Anuario de Derecho Constitucional Latinoamericano, Bogotá, 2020
DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

Herausforderungen des digitalen Zeitalters in einer hyperverlinkten Gesellschaft: der effektive Schutz der Menschenrechte in der Dominikanischen Republik

ZUSAMMENFASSUNG

Der technologische Fortschritt transformiert die heutige Realität. Information wird in kürzester Zeit übertragen. Die Verlinkung nimmt kontinuierlich zu, Daten werden zu äußerst wertvollen Aktivposten. Diese Situation ist mit juristischen Herausforderungen verbunden, da die einzelnen Grundrechte mit neuen Gegebenheiten konfrontiert werden, die rechtliche Transformationen erforderlich machen, um einen angemessenen Schutz zu gewährleisten, bei dem den Gerichten eine wesentliche Rolle zukommt.

Schlagwörter: Hyperverlinkung; Grundrechte; juristische Proaktivität.

Introducción: desafíos de la era digital en una sociedad hiperconectada y derechos fundamentales

Asistimos a una revolución tecnológica donde la esfera digital y las capacidades de cómputo crecen exponencialmente. Esto posibilita la hiperconectividad entre las personas y, en consecuencia, un gran flujo de información generador de datos que adquieren un valor sin precedentes, al punto de ir desplazando la economía tradicional hacia los recursos infinitos entre los que se encuentra la información. Su magnitud es tal, que el Foro Económico Mundial califica los datos como el petróleo del siglo XXI.[1]

La información que se despliega en la red refleja nuestros pensamientos y comportamientos más íntimos y profundos porque nos encontramos permanentemente conectados, permitiendo que las empresas y los Estados conozcan lo que hacemos o haremos siempre.[2]

El destacado historiador Yuval Noah Harari ha identificado la regulación de la propiedad de los datos como el mayor problema político, legal y filosófico de nuestra generación.[3] En el pasado fue sencillo delimitar la propiedad (vallas que separan y,

[1] Franklin Foer, *Un mundo sin ideas. La amenaza de las grandes empresas tecnológicas a nuestra identidad* (Barcelona: Espasa Libros, 2017); DerBlaueMond, "Data economy": Nuestros datos son la nueva materia prima de la economía, *World Economic Forum*, https://es.weforum.org/agenda/2017/05/data-economy-nuestros-datos-son-la-nueva-materia-prima-de-la-economia/.

[2] Paloma Lleneza, *Data Nomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos* (Barcelona: Editorial Planeta, S.A., 2019), 13.

[3] Cristina Galindo, "Yuval Noah Harari, el autor de 'Sapiens': «La tecnología permitirá 'hackear' a seres humanos»", *El País*, 29 de agosto de 2018, https://elpais.com/elpais/2018/08/20/eps/1534781175_639404.html.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

luego, títulos que te amparan). Sin embargo, la información digital plantea mayores dificultades, pues el contenido no depende del soporte físico y esto produce que puedan existir miles o millones de copias que estén en manos de otras personas o entidades una vez se generen.[4]

Según la Unión Internacional de Telecomunicaciones, en el año 2000 había 360 millones de personas conectadas a internet. Para 2005 la cifra alcanzaba los mil millones.[5] Actualmente, cerca de 5.19 mil millones de personas utilizan teléfonos móviles y 4.54 mil millones tienen acceso a internet, es decir, el 67 % de la población realiza interacciones múltiples que se registran en la red digital. La República Dominicana no es ajena a dicha situación, ya que en los últimos años se ha mantenido entre los países en vía de desarrollo con mayor nivel de crecimiento.[6]

Para solo citar un ejemplo, Mario Heidler Magallanes indica que, en 2016, ya el 82 % de nuestra población disponía de teléfono móvil.[7] Según el Fondo Monetario Internacional (FMI), la economía mundial creció 3,6 % en 2018 y 3,3 % en 2019, mientras que internet tiene un crecimiento del 7 % anual.[8]

Nelson José Guillén Bello, presidente del Instituto Dominicano de las Telecomunicaciones (Indotel), institución que regula este servicio en el país, señaló que el sector de las telecomunicaciones (digital) en 2018 aumentó 12,3 %, cifra superior a otros sectores, como el de la construcción, por lo que manifestó que "estamos cada vez más conectados entre nosotros y con el mundo".[9]

En efecto, el intercambio de datos se vuelve más dinámico porque la información se desplaza a la velocidad de la luz, lo que da lugar a que las personas tengan mayor acceso a la información y posibilidades de difusión. Sin embargo, junto con dichas oportunidades aumentan las capacidades de recolección y tratamiento de datos, tanto por la inmensidad de datos que se generan como por la existencia de más mecanismos y dispositivos para extraerla. Evidencia del referido escenario fueron las palabras del

---

4 Galindo, "Yuval Noah Harari, el autor de 'Sapiens': «la tecnología permitirá 'hackear' a seres humanos»".

5 Marc Goodman, *Delitos del futuro* (Barcelona: Ariel, 2015), 62.

6 Véase Banco Mundial, "República Dominicana: panorama general", https://www.bancomundial.org/es/country/dominicanrepublic/overview; Olga Bespalova y Marina Rosset, "Macrofinancial Linkages and Growth at Risk in the Dominican Republic", *IMF Working Papers* 19, n.º 246, November 13, 2019, https://www.imf.org/en/Publications/WP/Issues/2019/11/13/Macrofinancial-Linkages-and-Growth-at-Risk-in-the-Dominican-Republic-48792.

7 Mario Heidler Magallanes, "El fin de la privacidad: un acercamiento al pensamiento de Byung-Chul Han", *Global,* n.º 83 (2018): 67-71.

8 Fondo Monetario Internacional, *Informes de perspectivas económicas mundiales,* 19 de abril de 2019, https://www.imf.org/es/Publications/WEO/Issues/2019/10/01/world-economic-outlook-october-2019.

9 Dirección de Relaciones Públicas y Comunicaciones Indotel, "Indotel apostará por fortalecer la regulación del sector telecomunicaciones y digitalizar el país", 17 de mayo de 2019, https://www.indotel.gob.do/noticias/indotel-apostar%C3%A1-por-fortalecer-la-regulaci%C3%B3n-del-sector-telecomunicaciones-y-digitalizar-el-pa%C3%ADs/.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

director ejecutivo de Google, Eric Schmindt, cuando afirmó: "Desde el amanecer de la civilización hasta el 2003, se crearon más de 5 exabyte de información. En la actualidad, esta cantidad se está generando cada dos días".[10]

En este sentido, la información se convierte en un activo altamente preciado por la sociedad, razón por la que el mercado procura extraer el máximo beneficio económico con la hiperconexión digital para analizar los hábitos de los usuarios, buscando entrar así en lo más profundo de la psiquis humana.[11] De modo que para alcanzar su objetivo utilizan *software* de análisis cuantitativo que integran inteligencia artificial, aprendizaje automatizado, redes neuronales y algoritmos para construir una visión predictiva.[12]

En tales circunstancias, las personas se encuentran y dejan un rastro digital que forma parte de su personalidad y de los colectivos a los que pertenecen, lo que, posteriormente, posibilita que esa información pueda venderse. Las redes sociales constituyen un instrumento de la libertad de expresión, pues las publicaciones no solo tienen en cuenta momentos especiales (actividades festivas o viajes), sino que las personas son estimuladas para subir todo tipo de contenidos, hasta lo irrelevante o íntimo. En consecuencia, estas entidades editan según el tipo de personalidad que identifican con el objetivo de que utilicen la aplicación por más tiempo; por ende, la información consultada debe generar segregación de dopamina.[13] En efecto, las grandes plataformas digitales registran y procesan cada comentario, foto, video, me gusta, texto o el tiempo que duramos viendo una publicación para conocernos mejor y poder prever el comportamiento futuro.

Según Bynung Chung Han, destacado filósofo del pensamiento contemporáneo, la economía capitalista va adquiriendo un nuevo *modus operandi*, ya que, mediante la recolección y el tratamiento de datos, los Estados y las corporaciones pueden apropiarse de nuestros deseos, libertades y miedos.[14] Por tal razón, el derecho puede constituir un mecanismo para equilibrar los intereses involucrados, es decir, prerrogativas en conflicto para promover el bienestar humano a corto y largo plazo. Para alcanzarlo es preciso garantizar el manejo ético de la información personal, principalmente respecto a las esferas de intimidad.

Las empresas que operan bajo este nuevo formato económico son cada día más sólidas e imparables y su crecimiento parece no tener límites porque su activo

---

[10] Hugo Scolnik, *Qué es la seguridad informática* (Buenos Aires: Paidós, 2014).

[11] Marta García Aller, *El fin del mundo tal y como lo conocemos* (Barcelona: Editorial Planeta, 2017).

[12] Richard Kemp, "Big data and data protection (GDRP and DPA 2018)", Thomson Reuters Practical Law, https://uk.practicallaw.thomsonreuters.com/Document/I3cf592bad46211e8a-5b3e3d9e23d7429/View/FullText.html?contextData=(sc.Default)&transitionType=Default.

[13] Lucía Méndez, "La dopamina de las redes", *Elmundo.es*, 16 de diciembre de 2017, https://www.elmundo.es/opinion/2017/12/16/5a342ccce5fdea97248b4626.html.

[14] Lorenzo Cotino Hueso, "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata* 24, n.° 9 (2017): 79.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

principal es un recurso infinito (la información recopilada). Incluso se encuentran preparadas para subsistir ante crisis catastróficas. Por ejemplo, mientras escribo este trabajo, el mundo sufre una pandemia (el coronavirus o covid-19) que afecta directamente la economía mundial de manera drástica. Sin embargo, no dejamos de generar información, seguimos usando internet, redes sociales y teléfonos hasta más de lo habitual, algunos por miedo a la situación y otros por disponer de más tiempo de ocio, por ende, para recopilar más información.

El fundador y CEO de Facebook, Mark Zuckerberg, podría estar orquestando masivas pruebas aleatorias para evaluar cómo reaccionan las personas ante la crisis sanitaria actual porque el tránsito en la red ha crecido significativamente entre 25 y 40 %; este hecho permite captar más tiempo de atención y datos, y facilita entender las diferentes reacciones.[15] ¿Por qué puede convertirse en un problema? Porque el miedo nos deja más vulnerables y maleables frente a la comprensión de las conductas que alcanzan estas empresas y pueden derivar en una manipulación de las personas como sucedió en las elecciones presidenciales de Estados Unidos de 2016.[16]

La hipótesis anterior se sustenta en el hecho de que el efecto positivo o negativo de dichas herramientas tecnológicas dependerá de la finalidad para la que sean programados los sistemas que realizan la recolección y el tratamiento. Por ende, hay un condicionamiento respecto a los incentivos económicos que puedan existir. Siendo así, hay pocas posibilidades de que las entidades que acumulan y tratan los datos no se inmiscuyan en la vida privada de las personas y los utilicen a su favor, de lo que resultarán algunas recomendaciones legales que se harán más adelante.

Posiblemente surja la duda respecto a cómo la información de las personas se convierte en un activo valioso. Sin embargo, basta ver cómo aplicaciones gratuitas están valoradas en miles de millones de dólares. Tal es el caso de Facebook, que en 2014 se cotizaba en 200.000 millones de dólares, y cuatro años más tarde valía 420.000 millones de dólares.[17] La conclusión es clara: el negocio consiste en comercializar la información.[18]

---

[15] María Refojos, "Teletrabajo y ocio disparan el consumo de internet: ¿están las redes preparadas para el coronavirus?", *El Periódico*, 19 de marzo de 2020, https://byzness.elperiodico.com/es/innovadores/20200319/coronavirus-teletrabajo-ocio-consumo-internet-preparados-7895752.

[16] Luego de una investigación de la Cámara de Representantes de los Estados Unidos de América, se determinó que miles de anuncios en Facebook fueron puestos a circular por un grupo de rusos, quienes también crearon perfiles para apoyar los valores de uno de los candidatos de la contienda presidencial (Juan Martínez Martínez, "EE. UU. demuestra manipulación electoral a través de Facebook", *Vanguardia*, 15 de mayo de 2018, https://www.vanguardia.com/tecnologia/eeuu-demuestra-manipulacion-electoral-a-traves-de-facebook-EEVL433061).

[17] Fernando Galvan, "Instagram superó los 100 mil millones de dólares en valor de mercado", *merca20.com*, 25 de junio de 2018, https://www.merca20.com/instagram-supero-los-100-mil-millones-de-dolares-en-valor-de-mercado/.

[18] Goodman, *Delitos del futuro,* 153-154.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

Esto es posible gracias a que la cantidad de información que procesan ciertas entidades es inmensa. Esto sucede con Google, empresa que genera alrededor de un 1.000.000 de gigabytes por día; con un solo gigabyte, la capacidad de almacenar equivaldría a diez metros de libros colocados en un estante. Lo anterior significa que si toda la información procesada por esta corporación se imprimiera cada día y ese contenido se amontonara uno encima de otro, llegaría a alcanzar la mitad de la distancia que existe entre la Tierra y la Luna.[19] De allí que Google, mediante sus búsquedas gratuitas, alcanzara un valor de 400.000 millones de dólares en 2015,[20] crecimiento que parece no tener límites porque actualmente este alcanzó el trillón de dólares.[21]

El beneficio de dichas entidades es indiscutible porque han liberado la información a niveles exorbitantes, mejorando la conexión entre las personas y proporcionando cierta libertad de expresión. Pero la cuestión es cómo hacerlo sostenible a largo plazo y compatible con los valores democráticos y los derechos fundamentales. Contrario al mercado tradicional donde se intercambia un producto por una suma de dinero, en las plataformas digitales no existen consumidores convencionales; los clientes son consumidores y producto al mismo tiempo. A tal novedad se ha denominado técnicamente prosumidores por contar con características particulares frente al consumidor típico.

Esto significa que los usuarios participan directamente en el proceso de producción de los bienes y servicios que se comercializan. En otras palabras, son el producto de lo que supone un problema ético y jurídico que amerita atención y del cual ellos no están del todo enterados.[22]

Los entornos digitales no solo han generado controversia respecto a la finalidad con la que se usa la información personal, sino que también la hiperconexión ha derivado en una libertad de expresión que no tiene comparación histórica, empoderando a las personas hasta el punto de convertirse en un riesgo, en ciertas ocasiones, frente a derechos como el honor y la imagen personal. Debido a que la red facilita el acceso y la difusión de la información, ha aumentado la proliferación de mensajes de odio, incitación al crimen, robo de identidad y noticias falsas, jugando en contra nuestra y atacando principios fundamentales del Estado democrático de derecho. El ejemplo cumbre son las elecciones presidenciales de los Estados Unidos de 2016, donde Facebook y Cambridge Analytica usaron información personal para luego

---

[19] Goodman, *Delitos del futuro,* 84-86.

[20] Goodman, *Delitos del futuro,* 93.

[21] "Valor de Google supera el millón de millones de dólares", AM *México,* 17 de enero de 2020, https://www.am.com.mx/vivirmas/Valor-de-Google-supera-el-millon-de-millones-de-dolares-20200117-0017.html.

[22] Alvin Toffler y Heidi Toffler, *La revolución de la riqueza* (Ciudad de México: Editorial Random House Mondadori, 2006), 221.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

esparcir noticias falsas para convencer a los ciudadanos en función de las diferentes personalidades.[23]

Estas empresas tuvieron acceso a los datos personales de aproximadamente 85 millones de personas, valiéndose de las decisiones "libres" de sus usuarios, sin el consentimiento de la finalidad del tratamiento. Cabe destacar que las redes sociales están diseñadas para activar las mismas áreas cerebrales que drogas como la cocaína y crear formas de segregar dopamina (recompensa) por lo que producen dependencias psicológicas.[24] Incluso, según un artículo de *Forbes México*, la persona promedio consulta al menos 150 veces al día su móvil.[25]

En efecto, no solo se encuentra en riesgo la protección de la información personal, sino también la autonomía y libertad de las personas debido a que las redes sociales alcanzan su referido potencial porque los entornos digitales permiten economizar las pruebas de laboratorio. En la actualidad, entidades como Facebook hacen miles de pruebas aleatorias para analizar el comportamiento humano a una magnitud que en un día realizan más pruebas que la industria farmacéutica en un año.[26]

De modo que la situación se torna compleja porque la libertad de expresión (así como otros derechos impactados por los avances tecnológicos) se desprende del pluralismo cultural e ideológico que en el pasado fue tan vulnerado, pero hoy en día se encuentra contemplada en nuestras normas de mayor jerarquía. Alcanzar un equilibrio a través de regulaciones adaptadas a las nuevas realidades es uno de los grandes retos de estos tiempos.

La Corte Interamericana de Derechos Humanos (Corte IDH) ha querido aclarar este asunto, al afirmar que "el Estado debe de abstenerse con mayor rigor de establecer limitaciones a estas formas de expresión, […], en razón de la naturaleza pública de las funciones que cumplen, deben tener un mayor umbral de tolerancia ante la crítica".[27]

Indiscutiblemente, cuando la manifestación de la libertad de expresión se utilice para dirigirse a un funcionario público, la prerrogativa debe salvaguardarse en el sentido más amplio para evitar males peores. Sin embargo, el referido criterio solo abarca la postura que deben mostrar las instituciones estatales frente a los ciudadanos que usan las plataformas digitales para expresarse, pero no responde a las situaciones que pueden presentarse entre estos últimos.

---

[23] "Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios", *BBC News Mundo*, 29 de julio de 2019, https://www.bbc.com/mundo/noticias-49093124.

[24] Lleneza, *Data Nomics…,* 142.

[25] Rafael Solares, "La nomofobia: la adicción a nuestros celulares". *Forbes México,* 13 de marzo de 2018, https://www.forbes.com.mx/la-nomofobia-la-adiccion-a-nuestros-celulares/.

[26] Seth Stephens Davidowitz, *Todo el mundo miente* (Barcelona: Editorial Paidós, 2019), 131-132.

[27] Corte IDH, Caso Palamara Iribarne *vs*. Chile, Sentencia de 22 de noviembre de 2005, Fondo, Reparaciones y Costas, Serie C, núm. 135, 82.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

Las plataformas digitales, por su parte, han comenzado a censurar las publicaciones que puedan vulnerar derechos de otras personas, mensajes de odio o violación a la ley; sin embargo, cuando dichos mecanismos no funcionan, estos no comprometen su responsabilidad como en el caso de la prensa tradicional, tal como sucede en la legislación dominicana. En efecto, si estas aplicaciones, al igual que los medios tradicionales, editan la información, también deberían tener cierta obligación legal.

Por tal razón, los juristas deben comenzar a abordar las referidas cuestiones pues, de lo contrario, corren el riesgo de que el derecho quede rezagado frente a los avances tecnológicos, dejando en un campo de desprotección a las personas vulnerables.

Ante tal situación, es evidente que no se trata de una potestad del Estado, sino de una obligación a su cargo, porque todos los derechos indicados están contemplados en la Constitución. Efectivamente, en su artículo 38, la Constitución de la República establece que el Estado dominicano queda obligado a proporcionar las garantías suficientes para asegurar el respeto de los derechos fundamentales en general.[28] Por tal razón, no caben dudas de que el desafío del Estado es poner en equilibrio todos los derechos fundamentales que se encuentran involucrados y los grandes aportes de los avances tecnológicos porque se han convertido en parte de nuestras vidas.

De modo que para garantizar ese contrapeso entre derechos fundamentales y avances científicos y tecnológicos deben crearse regulaciones mediante las cuales los Estados adopten una visión global más allá del Estado-nación porque dicho sistema no se encuentra en condiciones de responder ante controversias que se extienden por todo el mundo, ya que no se creó para dichos fines. Las fronteras físicas son porosas en la esfera digital y van perdiendo su funcionalidad, es decir, no es efectivo regular tecnologías de implicación global desde el ámbito meramente nacional; en efecto, se necesita cooperación internacional.[29]

Para evidenciar el razonamiento anterior, basta ver la magnitud de algunas entidades digitales. Facebook dispone de 2.449 mil millones de usuarios; YouTube, 2.000 mil millones; Instagram, 1.000 mil millones; es de destacar que la más antigua de estas compañías tiene 16 años.[30] Esto significa que los usuarios de dichas plataformas se extienden por todo el mundo y, por ende, la vulneración de los derechos puede venir desde cualquier parte.

En este sentido, el impacto de las tecnologías de las telecomunicaciones amerita un enfoque diferente del derecho, que abarque el mayor número de variables, incluyendo la prevención de los sucesos que afectan derechos, porque en una sociedad hiperconectada que genera datos masivamente, el riesgo de posibles afectaciones es de gran magnitud y, por ende, no puede tratarse solamente de sancionar sino de prevenir.

---

[28] Constitución de la República Dominicana, proclamada el 13 de junio 2015.

[29] Goodman, *Delitos del futuro,* 18-19.

[30] Juan Carlos Mejía Llano, "Estadística de redes sociales 2020", 26 de febrero de 2020, https://www.juancmejia.com/marketing-digital/estadisticas-de-redes-sociales-usuarios-de-facebook-instagram-linkedin-twitter-whatsapp-y-otros-infografia/.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

1. El riesgo *vs*. la seguridad en la sociedad hiperconectada

En el presente escrito he mencionado que las tecnologías vinculadas a la esfera digital crecen exponencialmente porque operan en función de la ley de *Moore*, que establece que con el paso del tiempo la tecnología tiende a multiplicar su rendimiento y a dividir su coste. Esto implica que los dispositivos integrados a la red son cada vez más en cantidad, potencia y asequibilidad.[31] Dichas circunstancias crean un círculo masivo de producción de datos debido a la variedad de productos que recopilan información, lo que supone un aumento proporcional del riesgo.

Sin embargo, la cuestión no es que existan riesgos, sino la manera en que se gestionan. Actualmente, las entidades que realizan tratamiento de datos hacen dinero comercializando la información, no protegiéndola. Por tal razón, la seguridad de los datos no ha tenido la prioridad necesaria.

En este sentido, los riesgos son multidireccionales: primero, el hecho de que las entidades a quienes les confiamos los datos se benefician extrayendo el mayor número de información, de modo que si el negocio resulta rentable asumen el riesgo de tener que pagar multas exorbitantes. El Gobierno de Estados Unidos le impuso una multa de 5.000 millones de dólares a Facebook,[32] mientras que Google fue multada por el mismo monto en la Unión Europea; ambas por violación de privacidad; sin embargo, siguen siendo líderes dentro de su mercado. El segundo riesgo es la libertad que proporcionan dichos entornos, lo que genera la propagación de contenidos que afectan los derechos de terceros. Y el último es la facilidad con la que se filtra información.

La evidencia del tercer asunto propulsor de riesgo es la relativa facilidad con la que las grandes entidades digitales dejan filtrar información de sus usuarios por falta de medidas de seguridad. El departamento de seguridad de Facebook ha reconocido que se vulneran 600.000 mil cuentas cada día. En 2018, Facebook sufrió un ataque informático que dejó comprometida la información personal de posiblemente 90 millones de personas y propició que los *hackers* tuvieran acceso a las cámaras, micrófonos, archivos y fotos de los usuarios.[33]

En efecto, las personas se encuentran vulnerables no solo porque la mayoría de veces no proporcionan un consentimiento informado, sino también porque las entidades en las que depositan su confianza carecen de medidas de seguridad óptimas,

---

[31] Goodman, *Delitos del futuro,* 61-65.

[32] Namphi Rodríguez, "Gaceta Judicial. Redes sociales, campañas electorales y libertad de expresión: límites constitucionales", *Garcetas Judiciales*, n.º 386, 2019, 8. https://do.vlex.com/vid/redes-sociales-campanas-electorales-839612146?_ga=2.177582373.1850323928.1601907386-275380030.1601907386.

[33] Lleneza, *Data Nomics…*, 13.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

y permiten que se filtre información, es decir que terceros ajenos tengan acceso a la información de los usuarios.[34]

La era digital supone vivir en constante riesgo; así, el Servicio de Investigación del Congreso de Estados Unidos estimó que los fraudes vinculados con la identidad tuvieron un costo de 21.000 millones de dólares en 2012, cuyas víctimas fueron 13.1 millones.[35] Sin embargo, no se trata de una realidad aislada de los países desarrollados, ya que, según un artículo del *Diario Libre*, la República Dominicana se encuentra entre los países con mayor índice de robo de identidad; muestra de eso fue la cancelación de más de 13 mil cédulas por parte de la Junta Central Electoral en 2018, a causa de suplantación de identidad. La referida situación fue abordada en la conferencia "Nuevas tecnologías, seguridad jurídica y rol del notariado en el siglo XXI".[36]

Además, la esfera digital no se encuentra tan supervisada y regulada como los entornos tradicionales. Por ejemplo, Pro-Consumidor[37] no supervisa las aplicaciones que se comercializan a través de los celulares, lo que trae como resultado que el proceso de control quede en manos de los intereses privados y que el incentivo no sea la seguridad, sino la comercialización de la información.

En efecto, los algoritmos automatizados realizan el proceso de revisión sin mayores controles, lo que provoca la inexistencia de seguridad. En 2013, se detectaron aproximadamente 42.000 aplicaciones en la tienda de Google que tenían como objetivo espiar y robar información.[38] Sin embargo, esto no ha significado una carga de responsabilidad para dichas entidades, ni frente a las afectaciones ni respecto a las medidas de seguridad, porque siguen sin existir incentivos suficientes.

Por tal razón, no se trata de eliminar el riesgo sino de gestionarlo de manera que este se minimice. A estos fines, una de las formas de abordar el riesgo es a través de incentivos bidireccionales que consisten en fortalecer la protección de los datos para que las entidades ganen tanto comercializando la información como protegiéndola. En este sentido, si los jueces van construyendo un criterio sólido de lo que implica la obligación de seguridad, y también se construye un marco normativo adaptado a las realidades actuales, las entidades tendrán que invertir en seguridad.

El debate en torno a la era digital y sus riesgos amerita que las naciones dispongan de una entidad de control independiente que supervise a las entidades públicas

---

[34] Lleneza, *Data Nomics...,* 264 y 265.

[35] Goodman, *Delitos del futuro,* 157-159.

[36] "RD está en el top 10 de los países con robo de identidad, según especialista", *Diario Libre*, 7 de noviembre de 2019, https://www.diariolibre.com/actualidad/rd-esta-en-el-top-10-de-los-paises-con-robo-de-identidad-segun-especialista-PN15183518.

[37] Institución Nacional de Protección de los Derechos del Consumidor, establecida por la Ley 358-05, sobre protección al consumidor. Se encarga de salvaguardar las prerrogativas de los consumidores y usuarios de bienes y servicios, mediante la aplicación de las normas jurídicas establecidas y políticas.

[38] Goodman, *Delitos del futuro,* 187-189.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

y privadas para que tomen medidas de seguridad en función del riesgo que supone por el tipo de información que se encuentra en juego y por el volumen de esta. En este sentido, las medidas de seguridad deberían ser más altas para quienes dispongan de información sensible.

Sin embargo, en ninguna circunstancia dichas limitaciones pueden significar una coacción a la vida de las personas, es decir, su finalidad es garantizar el bienestar dentro de la sociedad democrática y de derecho, debido a que la potencia de los nuevos avances tecnológicos puede vulnerar los pilares que nos sostienen. Por tal razón, la seguridad opera como una herramienta para garantizar la dignidad humana a largo plazo, sin que los dispositivos que recopilan información desaparezcan, pero adecuándolos para los riesgos que suponen.

Resulta impresionante que para finales de 2020 se espera que existan 50.000 millones de dispositivos que se conecten a internet.[39] Esto abre la posibilidad de que se produzcan 2,5 septillones de interacciones de objeto a objeto, lo que generaría cantidades exorbitantes de datos dentro de un mayor número de esferas de la vida. Sin lugar a dudas, nuestro país debe prepararse no solo para lo que existe sino para lo que se aproxima.

Dichos dispositivos cuentan nuestros pasos, ritmo cardíaco, acceden a nuestra galería de fotos, graban nuestras conversaciones, registran los lugares a los que vamos, codifican nuestras medidas biométricas, la dilatación de las pupilas, ven contenido de preferencia, etc. De modo que toda esa información sensible debe disponer de controles que procuren su seguridad; porque si terceros sin principios acceden a ella, los daños pueden ser inmensos. Lo anterior, debido a que estas personas se dirigen donde se concentra la información, es decir, a las grandes entidades, por lo que pueden vulnerar los derechos de millones de personas simultáneamente.

En este sentido, si las empresas se benefician recolectando información y gracias a ello algunas entidades privadas están valoradas en miles de millones de dólares, entonces es más que prudente que los usuarios dispongan de garantías acordes con la naturaleza del tratamiento realizado, para que sus derechos estén protegidos y así se minimicen los efectos negativos, pues lo que se encuentra en juego no solo es nuestra intimidad sino también nuestra libertad y autonomía.

2. Los mecanismos de regulación del entorno digital

En la era digital, encontrar el equilibrio entre la protección de los datos personales, el acceso a la información, la libertad de expresión, el derecho al honor y a la imagen personal se convierte en un interés colectivo, sobre todo cuando están en juego datos sensibles que forman parte intrínseca de la personalidad de un individuo y

[39] Goodman, *Delitos del futuro,* 393.

DR © Konrad Adenaur Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

pueden vulnerar su dignidad o autonomía. El análisis de macrodatos[40] abre paso al escrutinio, la vigilancia y el análisis de gran parte de las interacciones humanas, debido a que nos encontramos conectados todo el tiempo, lo que expone nuestra esfera de intimidad a un nivel sin precedentes históricos, es decir, las personas se han convertido en máquinas de generación de datos.[41]

En la República Dominicana, prerrogativas como el derecho a la intimidad, el honor personal y la protección de datos tienen como punto de partida la Constitución y se encuentran conectadas, es decir, se contemplan de manera conjunta. La carta magna se encarga de hacer consistente la obligación de respetar la vida privada, abarcando la imagen propia, a través de su artículo 44, mientras que consagra la libertad de expresión e información en su artículo 49. A pesar de su consagración en el texto constitucional, se necesita de la promulgación de leyes especiales para garantizar estos derechos.

En la esfera nacional, el país dispone de la Ley 172-13, para la protección de la información personal, la intimidad, el honor, e incluso el mismo acceso a la información; la Ley 6132, que aborda la libertad de expresión y difusión del pensamiento; la Ley 200-04 de Acceso a la Información Pública; la Ley 53-07 sobre crímenes y delitos de alta tecnología, y la Ley 192-19 sobre la Protección de la imagen, el honor e intimidad familiar, vinculada a personas fallecidas y accidentadas.

No obstante, los mayores desafíos de la era digital recaen sobre la Ley 172-13, ya que su cuestionamiento parte de medidas que no necesariamente derivan en la responsabilidad penal de quien realiza el tratamiento de datos. Además, cuando las entidades reciben ataques verdaderamente delictivos no son penalmente responsables, pero en el escenario actual ni siquiera civilmente; este último aspecto es el que puede fortalecerse para alcanzar la seguridad que nuestra sociedad necesita.

En efecto, la protección de datos personales y sus derechos conexos requieren una normativa más robusta que amerita definiciones y principios que la complementen porque se ha visto muy afectada por el transcurso del tiempo. La Ley 172-13 integra una serie de principios: la licitud de archivos de datos personales, es decir, el fin no puede ser contrario a la ley; la calidad de los datos implica que la información debe ser cierta, adecuada y vinculada con la finalidad para la que fue recogida; el derecho a la información obliga a quien la recolecta a garantizar que los usuarios tengan el control (rectificación y supresión) sobre sus datos; el consentimiento del afectado; la seguridad de los datos; y el deber de secreto, en virtud de la esfera profesional en que se desarrolla la recolección de la información.[42]

---

[40] En el sector de las tecnologías de la información y de la comunicación, los macrodatos se refieren a un conjunto de datos que, por su volumen y variedad y por la velocidad a la que necesitan ser procesados, supera las capacidades de los sistemas informáticos habituales.

[41] Naciones Unidas, *Macrodatos para el desarrollo sostenible,* https://www.un.org/es/sections/issues-depth/big-data-sustainable-development/index.html.

[42] La Ley 172 de 15 de diciembre de 2013 tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

El consentimiento constituye uno de los ejes centrales para recolectar y tratar la información; este debe ser voluntario, inequívoco, libre, específico e informado.[43] En este aspecto, empieza la ineficiencia del marco normativo, como el de la República Dominicana, debido a que no existe un instrumento que obligue a las entidades que recolectan y tratan datos en la esfera digital a proporcionar garantías al respecto.

Según una investigación de Carnegie Mellon University en Estados Unidos, la persona promedio se topa con 1.462 políticas de privacidad al año, las cuales tienen un aproximado de 2.518 palabras, es decir que si las personas leyeran cada política de privacidad, deberían invertir 76 jornadas laborales de ocho horas.[44] Mientras que otra investigación enfocada en las políticas de privacidad de Apple, Amazon, Google, Facebook y Domino´s en conjunto contienen 76.069 palabras, que con un ritmo de lectura alto se necesitarían cinco horas de lectura continua; además, tendrían que releerla porque la actualizan constantemente.[45]

Esto significa que las personas están usando las diferentes aplicaciones o páginas de internet sin leer todas las políticas de privacidad porque no disponen del tiempo, lo que conlleva un consentimiento dado, pero no informado, ya que las personas carecen de la autonomía y conciencia necesarias, es decir, no saben o no entienden el alcance de derechos que están otorgando ni la forma en la que se utilizará su información personal. Se estima que aproximadamente el 72 % de la información que se recopila se hace sin que el usuario tenga conocimiento de ello, por ende, la entidad no cuenta con el consentimiento informado del titular de los datos (en otras palabras, del titular del derecho sobre estos).[46]

De acuerdo con el Grupo de Trabajo del artículo 29,[47] el consentimiento informado implica que el usuario debe conocer, claramente y mediante informaciones provistas por quien fuere a procesar sus datos, i) las empresas o personas que controlarán su información, ii) el objeto del procesamiento de los datos y para qué pide el consentimiento, iii) qué tipo de datos o informaciones serán recolectadas, iv) la posibilidad de retirar su consentimiento, y v) los riesgos que conlleva la transferencia y el procesamiento de sus datos personales.[48]

---

de tratamiento de datos destinados a dar informes, sean estos públicos o privados.

[43] Este es el estándar del consentimiento en la Unión Europea. Véase Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, artículo 4.11.

[44] Goodman, *Delitos del futuro,* 96.

[45] Lleneza, *Data Nomics…,* 48.

[46] Lleneza, *Data Nomics...,* 48.

[47] Se trató de una mesa de trabajo que dio soporte a la Unión Europea en la preparación de guías de las mejores prácticas para la protección de datos (https://edpb.europa.eu/our-work-tools/article-29-working-party_es).

[48] Comisión Europea, *Guidelines on Consent under Regulation 2016/679,* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

Lo más importante para asegurar que se trate de un consentimiento informado es que la regulación pueda garantizar que la información sobre el uso de los datos sea lo más sencilla y comprensible posible para el usuario.[49]

En adición, se encuentran las famosas *cookies*[50] que los usuarios se ven en la obligación de aceptar para usar las aplicaciones. Estas son archivos que se descargan en el dispositivo al acceder a una página de internet o aplicación, algunas son permanentes, otras temporales, y tienen como objetivo recolectar información del usuario mientras navega en la web o usa alguna aplicación cualquiera.[51]

Aunque se conozca qué son estos archivos, se ignora su finalidad exacta; en consecuencia, las personas y el propio Estado se encuentran en el mismo desconocimiento frente a los referidos instrumentos informáticos, lo que conforma una caja negra donde los usuarios no pueden saber si se respetan principios sobre protección de datos personales que consagra la ley.[52]

Ante dicha situación se encuentra más que justificado que las nuevas normativas que regulen las esferas digitales puedan contemplar límites en el número de palabras de las políticas de privacidad y, a su vez, la cantidad de veces que son actualizadas al año. La referida limitación pudiera establecer parámetros según el tipo de servicios o productos que preste la entidad, cuya finalidad sería colocar a los usuarios en una condición de leer las políticas de privacidad para que el consentimiento sea informado.

Nuestra ley nacional contempla los principios más conocidos de la protección de datos personales e integra definiciones para que sea clara y precisa. Sin embargo, no introduce las nuevas tecnologías en el proceso de protección, es decir, no existe la autorregulación. Esto significa que la finalidad normativa solo contempla solucionar situaciones con posterioridad a la afectación y no previniendo que se presente.

La referida situación es resultado de que el cambio revolucionario de las tecnologías de las telecomunicaciones no es contemplado por nuestra ley nacional, debido a que la ley de protección de datos personales (a pesar de ser de 2013) toma de referencia la Ley Orgánica 15/1999 de España, por lo que no contemplaba el escenario en el que nos encontramos, pues la esfera digital ha cambiado mucho desde entonces. Incluso en su país de origen ya fue sustituida por dicha razón.[53]

---

[49] Comisión Europea, *Guidelines on Consent under Regulation 2016/679*.

[50] Una *cookie* es un instrumento informático enviado por un sitio web y almacenado en el dispositivo del usuario, de manera que el sitio puede consultar las actividades previas o posteriores del usuario.

[51] Goodman, *Delitos del futuro,* 89-91.

[52] Goodman, *Delitos del futuro,* 89-91.

[53] Francisbel Jerez Castillo, "El reglamento general de protección de datos de la UE: un espejo en el que debemos mirarnos", *Diario Libre,* 29 de mayo de 2015, https://www.diariolibre.com/opinion/en-directo/el-reglamento-general-de-proteccion-de-datos-de-la-ue-un-espejo-en-el-que-debemos-mirarnos-IM12879809.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

Si bien es cierto que en el ámbito nacional, al detectar situaciones que violentan sus derechos, los usuarios pueden accionar para rectificar, cancelar o efectuar una oposición respecto a la información que los afecta, no menos cierto es que con ese *modus operandi* no es suficiente. Las grandes entidades privadas no dejan filtrar fácilmente sus propias injerencias y, por lo tanto, es difícil para los usuarios probarlo.

En consecuencia, necesitamos introducir en nuestra regulación mecanismos de autorregulación que permitan una protección más dinámica y un derecho proactivo que, en primer lugar, eviten las afectaciones. La cuestión consiste en cómo crear una estructura garantista frente a una sociedad de riesgo constante.

Debido a que la finalidad es visualizar la realidad dominicana solo identificaré los aspectos que puedan constituir un beneficio y una adecuación de la normativa nacional frente a la realidad actual. Dentro de estos se encuentra la privacidad por diseño y por defecto que consiste en que las empresas y personas que fabrican nuevas tecnologías revistan sus programaciones o sistemas con valores éticos, como el principio de beneficencia y no maleficencia, para que sean respetadas las esferas privadas o íntimas de los usuarios, minimizando así el impacto negativo del tratamiento de datos. Esto implica, a su vez, evaluar los riesgos y tomar medidas objetivas para abordarlo; en caso contrario, la entidad comprometería su responsabilidad.

Evidentemente, esto daría lugar, en algún sentido, a una limitación a la libertad de empresa o, más bien, este tipo de política regulatoria podría afectar dicho derecho fundamental. Sin embargo, como ya ha considerado el Tribunal Constitucional,

> el derecho a la libertad de empresa, como derecho fundamental, se configura como un derecho que solo puede ejercitarse en el mercado, que consiste en la libertad para decidir qué producir y cómo hacerlo de acuerdo con la ley. El valor jurídico protegido por la libertad de empresa es la iniciativa económica privada como elemento esencial de una economía de mercado, libertad que sólo podría estar limitada, de acuerdo con el citado artículo 50 de la Constitución, por las disposiciones contenidas en la Constitución y las leyes.[54]

De modo que este tipo de regulación puede incorporarse al quehacer de las empresas, siempre y cuando esté prevista en una ley, mecanismo normativo constitucionalmente previsto para limitar los derechos fundamentales conforme al artículo 74.2 de la Constitución de la República Dominicana.

Por demás, la práctica de la privacidad, por diseño y por defecto, encuentra su experiencia comparada en el Reglamento General de Protección de Datos de la Unión Europea, que intenta dar un giro mayor de protección a los datos personales, en tanto pone en manos de las empresas idear los mecanismos más adecuados para proactivamente procurar una efectiva protección de datos, como sucede también con las normativas tendientes al cuidado del medioambiente.

[54] Tribunal Constitucional, TC/0535/15, párr. 11.21.

DR © Konrad Adenaur Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

En efecto, lo anterior tiene un carácter preventivo y proactivo en el sentido de que no procura sanción, sino que los hechos ilegítimos no acontezcan como sucede con el principio de precaución del derecho ambiental, pero dentro del entorno digital.[55] Dichas medidas de seguridad deben ser proporcionales al tipo de información que maneje la entidad.

La privacidad por diseño y defecto se vincula con las evaluaciones de impacto, ya que para que pueda existir la primera debe preverse la segunda. Este tipo de evaluaciones identifica los riesgos probables o posibles de un tratamiento para luego proceder a erradicarlos o limitarlos antes de que surjan hechos gravosos; además, procura simultáneamente transparentar los procesos tecnológicos, es decir, saber el contenido esencial de los sistemas informáticos.[56]

Por ejemplo, en una máquina de hacer café que tiene diferentes botones, uno de ellos para capuchino, cada vez que presionas esa función tendrás el mismo resultado, debido a que la programación que dispone ese sistema opera en función de algoritmos (conjunto de operaciones que se llevan a cabo para realizar la tarea en cuestión); de esa misma manera pueden instalarse algoritmos éticos para que cada vez que se realice un tratamiento de datos, la esfera privada se encuentre protegida.

El análisis del impacto no solo constituye un principio, sino también una obligación a cargo del responsable del tratamiento, al menos en el marco jurídico de protección de datos de la Unión Europea,[57] que nos sirve como apoyo en este análisis. A este compromiso se le denomina responsabilidad proactiva. Por lo tanto, su incumplimiento constituye una falta y si ese comportamiento antijurídico genera daño, entonces, el responsable compromete su responsabilidad.

El complemento de dichas previsiones legales son los códigos de conducta, que consisten en una reglamentación interna que deben usar las entidades como garantía de cumplimiento de requerimientos legales. Allí se identifican las formas en que se pretende operar, de manera que el sistema sea seguro para que exista dicho instrumento que debe ser integrado en el marco normativo. Esto facilita identificar si la empresa, en caso de violación, actuó acorde con el protocolo establecido.

Sin embargo, para que las instituciones públicas y privadas se vean incentivadas a disponer de tal instrumento, las normativas relativas a los entornos digitales deben integrar el principio de precaución, propio del derecho ambiental; así se construye la obligación de asumir una serie de medidas preventivas para quien se beneficia del tratamiento en este caso.

---

[55] Rosario Duaso Calés, "Los principios de protección de datos desde el diseño y protección de datos por defecto", en *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de protección de datos*, ed. por José Luis Piñar Mañas (Madrid: Reus, 2016), 295-320.

[56] Luis Felipe López Álvarez, "La responsabilidad del responsable", en *Reglamento general de protección de datos…*, 275-289.

[57] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, artículo 35.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

Evidentemente, la normativa nacional en virtud de los aspectos indicados previamente tiene precariedades. Dentro de ellas, estar enfocada en los servicios crediticios, lo que se confirma con el artículo 29 de la Ley 172-13, el cual establece como órgano de control a la Superintendencia de Bancos.[58]

En definitiva, la normativa nacional debe hacer suyas las actualizaciones recomendadas, integrando, por lo menos, dos elementos. El primero, consiste en crear instrumentos jurídicos de cooperación internacional o en bloque fundamentado en principios y valores comunes como mecanismo de presión para garantizar la privacidad por diseño de los avances tecnológicos. En segundo lugar, el Estado debe promover e implementar políticas que saquen a la población del analfabetismo informático porque los usuarios deben concientizarse para que los ajustes sean más efectivos. Una muestra de dicho déficit son las votaciones internas simultáneas de los partidos políticos del 6 de octubre de 2019 para escoger los candidatos de elección popular, donde el voto automatizado ralentizó el proceso de votación porque algunos ciudadanos no estaban familiarizados.[59]

3. El papel jurisdiccional frente a los desafíos de la era digital

Los derechos fundamentales abordados en el presente ensayo, como libertad de expresión, intimidad, protección de datos personales, acceso a la información y derecho al honor, en ocasiones pueden resultar contradictorios y entrar en conflicto entre sí, sobre todo porque actualmente está bastante difundida y asentada la idea de que los derechos fundamentales entran en conflicto cuando se trata de su vigencia práctica.[60] Sin embargo, la Constitución de la República es un instrumento pluralista, es decir, contempla principios, valores, prerrogativas y reglas diversos que favorecen la cohesión social. De modo que cuando se presentan conflictos de derechos fundamentales, al no existir jerarquización, los jueces ponderan el derecho que amerita ser prioritario. En este sentido, se ha expresado el criterio del Tribunal Constitucional español: "Recuerda que no existe una relación de jerarquía, como en

---

[58] Carlos Pérez Tejada, "¿Quién hace negocio con tu data personal?", *Diario Libre*, 11 de junio de 2019, https://www.diariolibre.com/estilos/blogs/martes-de-tecnologia/quien-hace-negocio-con-tu-data-personal-EB13034220.

[59] Odalis Mejía, "En Santo Domingo participación masiva, pero proceso fue lento", *Hoy,* 7 de octubre de 2019, https://hoy.com.do/en-santo-domingo-participacion-masiva-pero-proceso-fue-lento/.

[60] Luis Fernando Castillo Córdova, "¿Existen los llamados conflictos entre derechos fundamentales?", *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional,* n.° 12 (2005), https://revistas.juridicas.unam.mx/index.php/cuestiones-constitucionales/article/view/5726/7511.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

el caso del derecho a la intimidad, entre las libertades de expresión e información y el derecho fundamental a la protección de datos personales".[61]

En efecto, el papel jurisdiccional es de alta importancia porque ante los conflictos de derechos fundamentales permite adaptar las prerrogativas en virtud de las circunstancias particulares. En este sentido, dicho proceso interpretativo esclarece la aplicación del marco normativo y, a su vez, construye referencias para futuras situaciones. En la República Dominicana, la función se dificulta porque no existe un órgano de control que le facilite el trabajo; además, respecto a la protección de datos personales y derechos conexos debe interpretarse una norma enfocada en las entidades crediticias, a pesar de que la realidad social es más amplia.

Frente a tales limitaciones, el Tribunal Constitucional ha aplicado la normativa en un sentido amplio, fortaleciendo el criterio de que en aquellas situaciones donde se opera sin el consentimiento del titular de los datos o se dispone de una información errónea, este puede accionar en *habeas data*, en caso de ausencia de respuesta.[62]

Sin embargo, la función de los tribunales como órganos de control surge con posterioridad a la vulneración de derechos. Por ende, no hay un control *ex ante* que permita supervisar preventivamente las medidas de seguridad aplicadas por las plataformas digitales frente a derechos fundamentales en riesgo con su interacción en el entorno digital. De ahí que se requiere un regulador, un ente estatal más robusto que, previa conculcación de derechos, intervenga, dados los elevados riegos en el ciberespacio. Aunque inexistentes en la actualidad, hay que valerse de instrumentos de prevención estatales, pues las facultades de Indotel, ente naturalmente inclinado a la protección de datos en el entorno digital, no tienen el alcance adecuado. Esto, en parte, porque la Ley General de Telecomunicación (Ley 153-98) es de 1998, es decir que su actualización es imperativa, en conjunto con la actual ley de protección de datos antes mencionada, para abordar adecuadamente el entorno digital y garantizar una mejor y efectiva protección de los derechos fundamentales.

A pesar de lo indicado, el Tribunal Constitucional ha mostrado dentro de su función y posibilidades ser un verdadero garante del derecho a la intimidad, tal como lo evidencia su postura cuando tuvo que referirse a la Resolución 086-11 de 1 de septiembre de 2011, emitida por Indotel,[63] cuya finalidad era permitir el acceso a la información de las personas sin orden judicial previa. Múltiples artículos de dicha resolución fueron declarados inconstitucionales en 2013 por transgredir la esfera privada sin la confirmación de elementos que lo justificasen.[64]

---

[61] Tribunal Constitucional de España, STC 155/2009 de 18 de mayo.

[62] Tribunal Constitucional de la República Dominicana, Sentencia TC/0334/17.

[63] Instituto Dominicano de las Telecomunicaciones (Indotel), Resolución 086-11 de 1 de septiembre de 2011, que aprueba el reglamento para la obtención y preservación de datos e informaciones por parte de los proveedores de servicios, en aplicación de las disposiciones de la Ley 53-07 sobre crímenes y delitos de alta tecnología.

[64] Tribunal Constitucional de la República Dominicana, Sentencia TC/0200/13.

DR © Konrad Adenaur Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

Igualmente, el Tribunal Constitucional prioriza el acceso a la información de los individuos frente al Estado en lo relativo a datos de interés público. La evidencia es el criterio sostenido en ocasión de una acción de amparo contra el Ministerio de Defensa, donde indicó que el derecho al libre acceso a la información pública tiene la finalidad de "controlar el uso y manejo de los recursos públicos y, en consecuencia, ponerle obstáculos a la corrupción administrativa", interpretación reforzada por la Sentencia TC/0062/13 donde se reconoce valor del derecho a la intimidad y protección de datos personales, pero no frente a los intereses públicos, es decir que solo cuando no existe tal característica se priorizada la esfera privada.[65]

Sin embargo, pueden presentarse situaciones que ameriten el acceso a la información y la protección de datos personales (incluyendo intimidad). En tales circunstancias, las limitaciones de ambos derechos pueden ser parciales, es decir, restringirse la información irrelevante para los fines deseados o que sean de interés meramente privado. Por ejemplo, ante la pandemia del covid-19, las instituciones estatales publican el número de contagiados por zonas y del territorio nacional (información imprescindible para mantener a la ciudadanía informada). Sin embargo, no se identifica a los afectados a pesar de que las autoridades sí tienen los datos personales de los individuos infectados, pues los laboratorios y hospitales están obligados a suministrarlos.

Hay situaciones donde resulta más difícil identificar qué derecho debe ser priorizado o cómo proceder con limitaciones parciales, en cuyo caso se recurre a principios constitucionales como el de proporcionalidad para establecer si la publicación de los datos o accesibilidad de estos constituye una medida indispensable para salvaguardar el interés público.[66] De modo que se debe tomar en cuenta la finalidad, la necesidad e idoneidad para establecer la justificación que motiva la restricción de un derecho u otro, dependiendo del caso.

La Sala Constitucional de la Corte Suprema de Justicia de Costa Rica ha establecido que la necesidad en el referido contexto se refiere a la base fáctica o circunstancias que hace preciso proteger algún bien o colectividad de bienes jurídicos, es decir que si la medida no se realiza, el interés público se ve afectado; mientras que la idoneidad constituye la forma en que se pretende resolver la necesidad detectada; por último, lo anterior se justifica siempre y cuando la solución sea proporcional.[67]

El hecho de disponer de los referidos principios para proporcionar respuestas se encuentra relacionado con lo que Ronald Dworkin expresa en el sentido de que las personas tienen derechos, cuando no existe una meta colectiva que justifique

---

[65] Tribunal Constitucional de la República Dominicana, Sentencia TC/0062/13.

[66] Centro de Información Jurídica en Línea del Colegio de Abogados de Costa Rica, *Principios constitucionales de razonabilidad y proporcionalidad,* https://cijulenlinea.ucr.ac.cr/portal/descargar.php?q=NDg4, 11-12.

[67] Sala Constitucional de la Corte Suprema de Justicia de Costa Rica, Sentencia 08858-98 de 15 de diciembre de 1998.

DR © Konrad Adenaur Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

negárselos.[68] De modo que la tendencia del Estado debe ser la de permitir el acceso a la información pública porque con ello indirectamente salvaguarda un interés público, mientras que frente a aquella información de índole meramente personal y privada debe primar la protección de datos personales porque, en la era digital, las herramientas de seguridad ante el riesgo de manejo inadecuado de las informaciones personales justifican la restricción de los datos personales.

De modo que el ideal es garantizar la mayor transparencia posible de la administración pública para que quienes eligen a sus representantes tomen mejores decisiones para el buen funcionamiento del Estado democrático. Por otro lado, frente a instituciones privadas o datos sensibles e íntimos, se requieren herramientas que procuren su protección y una tutela judicial efectiva que garantice los derechos fundamentales a la intimidad y el honor.

Frente a intereses meramente privados siempre debe protegerse tanto el derecho a la intimidad como los datos personales. Es importante tomar en cuenta que el límite del derecho a la información es marcado, precisamente, por el derecho a la intimidad y a la protección de datos personales, de modo que, tal como ha señalado el Tribunal Constitucional, resultaría violatorio de estos últimos la divulgación de información que "carezca de incidencia en asuntos de interés colectivos".[69]

Sin embargo, en las esferas digitales no resulta tan sencillo percibir las injerencias a la vida privada porque suceden en un escenario intangible. De modo que el referido criterio, aunque parece bastante garantista, contiene precariedades frente a las plataformas digitales. Por tal razón, los tribunales aún tienen margen de acción, es decir, pueden establecer límites a la extensión de las políticas de privacidad para que los usuarios se encuentren en condiciones de leerlas. De modo que utilicen la función jurisdiccional para seguir el ritmo de los avances tecnológicos ante la lentitud de las modificaciones normativas con lo cual se podría empezar a afrontar la situación, siempre que en sus decisiones los tribunales construyan sólidamente sus fundamentos y estas no adolezcan de falta de motivación.

La jurisprudencia ha establecido que los datos personales son toda aquella información que permite identificar a una persona de forma directa o indirecta, independientemente del soporte en el que se encuentre el contenido[70] y, por ende, son una extensión de la persona, por lo que es preciso preguntarse a quién le corresponde el control de la información. En este sentido, el Poder Judicial, en virtud de las leyes preexistentes, puede establecer criterios interpretativos mediante sus sentencias, donde se identifiquen las implicaciones de las obligaciones de las partes.

---

[68] Laura Nahabetián Brunet, *Protección de datos personales vs. acceso a la información pública. ¿Derechos fundamentales en conflicto?*, 11, http://www2.congreso.gob.pe/sicr/cendocbib/con2_uibd.nsf/C43D4582907B5890052578080076 3C5A/%24FILE/nahabetian.pdf.

[69] Tribunal Constitucional de la República Dominicana, Sentencia TC/0011/12.

[70] Ana Garriga Domínguez, *Nuevos retos para la protección de datos personales en la era del big data y la computación ubicua* (Madrid: Dykinson, 2016), 168.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

En efecto, la jurisprudencia puede fortalecer las implicaciones derivadas de las obligaciones consagradas por la ley, es decir, llenarlas de un contenido que encomiende medidas principalmente al responsable del tratamiento. Cabe destacar que en la recolección y el tratamiento de datos existe la obligación de seguridad[71] por parte del responsable del tratamiento. Dicha situación proporciona otra oportunidad a los jueces para dotar de mayor contenido el alcance de la obligación de seguridad que tienen los responsables del tratamiento de datos e informaciones personales, tal sería tener como estándar la encriptación de datos como forma de garantizar mayor seguridad de los datos y minimizar el riesgo de filtraciones y hackeos a los usuarios.

La encriptación consiste en un mecanismo para asegurar la confidencialidad en la esfera digital. Dicho proceso podría formar parte de la obligación de seguridad que debe proporcionar quien realiza el tratamiento de datos, pues implicaría que las empresas deben hacer todo lo posible por proteger los datos de sus contrapartes, es decir, tomar todas las medidas de seguridad posibles para evitar daños a sus usuarios y clientes.

De modo que al poder ser una obligación de seguridad, no es de extrañar que, ante los tribunales, la carga de la prueba sea a la inversa, es decir que el responsable del tratamiento de los datos sea el que debe probar que cumplió con todos los requerimientos de protección previstos en las normas vigentes, sobre todo en aquellos casos donde se trate de información sensible o protegida debido a los riesgos que supone frente a diversos derechos fundamentales.[72]

Dicha situación podría potenciar el mercado de la seguridad de los datos porque las entidades se verían obligadas a invertir más en ciberseguridad; por ende, quienes se dedican a dicha área tendrían mayor demanda, lo que conduciría al crecimiento del sector.

El criterio anterior permitiría expandir dicho mercado, lo que generaría beneficios económicos y sociales, al igual que cuando se impusieron los seguros obligatorios para los vehículos de motor. Como se ha planteado, en la actualidad vivimos en una sociedad de riesgo debido a la hiperconexión, que desencadena un flujo masivo de información e interacciones. En este sentido, el Poder Judicial debe disponer de las herramientas que faciliten las condiciones necesarias para que las personas gocen de la tutela judicial efectiva.

Sin embargo, al Poder Judicial no le bastaría con robustecer sus criterios, ya que cuando las afectaciones se confirman no solo es necesario tener un soporte interpretativo del cual disponer porque parte del problema es la lentitud con la que opera el

---

[71] La obligación de seguridad consiste en tomar medidas razonables de custodia y vigilancia para prevenir y evitar los daños a la contraparte, lo que no puede reputarse como extraño a la actividad de la empresa [Jorge Subero Isa, *Tratado práctico de responsabilidad civil dominicana* (Santo Domingo: Corripio, 2018), 311].

[72] Corte de Casación (Francia), *Maritime Trasatlantique vs Hamida Ben Mahmoud*, 21 de noviembre de 1911.

Anuario de Derecho Constitucional Latinoamericano, Bogotá, 2020
DR © Konrad Adenaur Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

proceso judicial para proporcionar una respuesta. De ahí que se vulnere el derecho de las personas a recibir una justicia pronta, oportuna y efectiva.

En efecto, el Poder Judicial necesita asistencia de un órgano de control que tenga potestad de realizar ciertas gestiones de manera más rápida, supervisando y aplicando las normas de protección de datos y, a su vez, recibiendo las reclamaciones de los afectados. Esto permitiría que el proceso pudiera resolverse antes de judicializarse y, en caso contrario, la jurisdicción contara con mayores precisiones sobre la situación porque dicha entidad también supervisaría y recibiría las reclamaciones.

Conclusiones: ¿qué podemos hacer para el mejoramiento del entorno digital?

En la era digital, como se ha podido contemplar, existen grandes desafíos porque hay involucrados intereses de todo tipo. Actualmente, quizás el enfoque óptimo sería buscar la combinación entre libertad, protección de datos y transparencia, sostenido, a su vez, en la cooperación internacional.

Sin embargo, cabe destacar que el mayor reto que acarrea la presente era digital son los asuntos relacionados con la intimidad de las personas. Dicho asunto es tan delicado porque si las entidades públicas o privadas se apropian del flujo masivo de datos y, con ello, de la parte íntima de las personas, se pone en juego su autonomía porque dicho conocimiento abre paso a la manipulación.

A pesar de que las referidas prerrogativas pueden entrar en conflicto, eso no imposibilita su convivencia. En efecto, para desarrollar un marco normativo garantista bajo el enfoque mencionado es preciso identificar cuándo existen intereses públicos o privados.

Los juristas deben ser fuente generadora de razonamientos legales que permitan abordar eficientemente el impacto social de la era digital porque el derecho como ciencia social se debe a las necesidades existentes. Por tal razón, los Estados deben garantizar la transparencia de las programaciones, evitando que ellas causen discriminaciones; de ahí la necesidad de valores éticos integrados a los sistemas.

Las nuevas normativas tendientes a salvaguardar la intimidad, el honor y la libertad de las personas necesitan transparentar el diseño para que los usuarios, a través de la información, se encuentren más empoderados. El mismo interés público permite entender que quienes se beneficien del tratamiento deben asumir parte de la responsabilidad por no haber contemplado una evolución de riesgos y medidas de seguridad derivadas de dicho análisis, ya que los usuarios son quienes depositan su confianza en sus productos o servicios y quienes cada vez se encuentran más conectados.

Las referidas medidas obligarían a las entidades a optar por dos opciones: la primera, invertir más en seguridad de manera directa; y la segunda, externalizar dicha obligación. En ambos casos, el mercado de seguridad podría crecer, lo que

DR © Konrad Adenaur Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

se traduciría en bienestar humano y económico, es decir, podría aportar beneficios para los intereses particulares y colectivos a la vez.

El presente ensayo ha tenido por finalidad identificar los puntos controvertidos que ameritan mayor atención de cara a los entornos digitales si queremos preservar la sociedad democrática y de derecho tal como la conocemos; además, la reflexión nos prepara para el futuro. ¿En realidad está en juego la democracia? El Tribunal Constitucional alemán concibe el derecho a la intimidad y protección de datos personales como una condición elemental dentro de una democracia en libertad fundada en la capacidad de acción de las personas.[73] No obstante, también la libertad de expresión y el acceso a la información son imprescindibles en el sistema democrático de derecho.

En consecuencia, debemos dirigir adecuadamente los avances tecnológicos digitales de manera que la autonomía de las personas no se ponga en juego y se garantice siempre el bienestar humano, para lo cual se necesita crear las condiciones que faciliten que la libertad de expresión y la protección de la información convivan de manera productiva dentro de una sociedad hiperconectada y en riesgo.

Estamos frente a una obligación de protección por parte del Estado, según lo establece la propia Constitución en su artículo 8 como función esencial del Estado, esto es, la protección efectiva de los derechos de la persona, para lo cual "se deben aplicar medidas progresivas que se adapten a las circunstancias para mantener los derechos revestidos de una protección eficiente".[74]

De modo que para evitar o minimizar los efectos negativos de la era digital con miras al bienestar colectivo, salvaguardando las libertades individuales de las personas, ante el riesgo de la carencia de consentimiento, tratamiento de datos masivos, manipulación e incluso dictaduras digitales (que la información se concentre en pocas entidades), necesitamos conocer con profundidad las implicaciones de la revolución digital en lugar de enfrentarla y con ello lograr que los programas y algoritmos digitales dispongan de los valores adecuados ya que significarían una mejora importante para nuestra sociedad, al tiempo que fortalecemos el marco legal que evitaría que las tendencias actuales resulten en catástrofes.[75]

Bibliografía

"Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios". *BBC News Mundo,* 29 de julio de 2019. https://www.bbc.com/mundo/noticias-49093124.

[73] Eduardo Jorge Prats, *Derecho constitucional,* volumen II (Santo Domingo: Ius Novum, 2016), 240.

[74] Prats, *Derecho constitucional,* 245.

[75] Yuval Noah Harari, *21 lecciones para el siglo XXI* (Barcelona: Editorial Penguin Random House, 2019), 85.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

"RD está en el top 10 de los países con robo de identidad, según especialista. 2019". *Diario Libre,* 7 de noviembre de 2019. https://www.diariolibre.com/actualidad/rd-esta-en-el-top-10-de-los-paises-con-robo-de-identidad-segun-especialista-PN15183518.

Castillo Córdova, Luis Fernando. "¿Existen los llamados conflictos entre derechos fundamentales?". *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*, n.º 12 (2005): 99-129. https://revistas.juridicas.unam.mx/index.php/cuestiones-constitucionales/article/view/5726/7511.

Centro de Información Jurídica en Línea del Colegio de Abogados de Costa Rica. "Principios constitucionales de razonabilidad y proporcionalidad". https://cijulenlinea.ucr.ac.cr/portal/descargar.php?q=NDg4.

Cotino Hueso, Lorenzo. "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales". *Dilemata* 24, n.º 9 (2017): 131-150.

Davidowitz, Seth Stephens. *Todo el mundo miente.* Barcelona: Editorial Paidós, 2019.

DerBlaueMond. "'Data economy': Nuestros datos son la nueva materia prima de la economía". *World Economic Forum*. https://es.weforum.org/agenda/2017/05/data-economy-nuestros-datos-son-la-nueva-materia-prima-de-la-economia/.

Dirección de Relaciones Públicas y Comunicaciones Indotel. "Indotel apostará por fortalecer la regulación del sector telecomunicaciones y digitalizar el país", 17 de mayo de 2019. https://www.indotel.gob.do/noticias/indotel-apostar%C3%A1-por-fortalecer-la-regulaci%C3%B3n-del-sector-telecomunicaciones-y-digitalizar-el-pa%C3%ADs/.

Duaso Calés, Rosario. "Los principios de protección de datos desde el diseño y protección de datos por defecto". En *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de protección de datos.* Editado por José Luis Piñar Mañas, 295-320. Madrid: Reus, 2016.

Foer, Franklin. *Un mundo sin ideas. La amenaza de las grandes empresas tecnológicas a nuestra identidad.* Barcelona: Espasa Libros, 2017.

Fondo Monetario Internacional. "Informes de perspectivas económicas mundiales del 19 de abril de 2019". https://www.imf.org/es/Publications/WEO/Issues/2019/10/01/world-economic-outlook-october-2019.

Galindo, Cristina. "Yuval Noah Harari, el autor de 'Sapiens': «La tecnología permitirá 'hackear' a seres humanos»". *El País*, 29 de agosto de 2018. https://elpais.com/elpais/2018/08/20/eps/1534781175_639404.html.

Galvan, Fernando. "Instagram superó los 100 mil millones de dólares en valor de mercado". *merca20.com,* 25 de junio de 2018. https://www.merca20.com/instagram-supero-los-100-mil-millones-de-dolares-en-valor-de-mercado/.

García Aller, Marta. *El fin del mundo tal y como lo conocemos.* Barcelona: Editorial Planeta, 2017.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

Garriga Domínguez, Ana. *Nuevos retos para la protección de datos personales en la era del big data y la computación ubicua.* Madrid: Dyckson, 2016.

Goodman, Marc. *Delitos del futuro.* Barcelona: Ariel, 2015.

Harari, Yuval Noah. *21 lecciones para el siglo XXI.* Barcelona: Editorial Penguin Random House, 2019.

Heidler Magallanes, Mario. "El fin de la privacidad: un acercamiento al pensamiento de Byung-Chul Han". *Global,* n.º 83 (2018): 67-71.

Jerez Castillo, Francisbel. "El Reglamento General de Protección de Datos de la UE: un espejo en el que debemos mirarnos". *Diario Libre,* 29 de mayo de 2015. https://www.diariolibre.com/opinion/en-directo/el-reglamento-general-de-proteccion-de-datos-de-la-ue-un-espejo-en-el-que-debemos-mirarnos-IM12879809.

Kemp, Richard. "Big data and data protection (GDPR and DPA 2018)". *Thomson Reuters Practical Law,* https://uk.practicallaw.thomsonreuters.com/Document/I3cf592bad46211e8a5b3e3d9e23d7429/View/FullText.html?contextData=(sc.Default)&transitionType=Default.

Lleneza, Paloma. *Data Nomics. Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos.* Barcelona: Editorial Planeta, 2019.

López Álvarez, Luis Felipe. "La responsabilidad del responsable". En *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de protección de datos*. Editado por José Luis Piñar Mañas, 275-289. Madrid: Reus, 2016.

Martínez Martínez, Juan. "EE. UU. demuestra manipulación electoral a través de Facebook". *Vanguardia*. 15 de mayo de 2018. https://www.vanguardia.com/tecnologia/eeuu-demuestra-manipulacion-electoral-a-traves-de-facebook-EEVL433061.

Mejía Llano, Juan Carlos. "Estadística de redes sociales 2020", 26 de febrero de 2020. https://www.juancmejia.com/marketing-digital/estadisticas-de-redes-sociales-usuarios-de-facebook-instagram-linkedin-twitter-whatsapp-y-otros-infografia/.

Mejía, Odalis. "En Santo Domingo participación masiva, pero proceso fue lento". *Hoy,* 7 de octubre de 2019. https://hoy.com.do/en-santo-domingo-participacion-masiva-pero-proceso-fue-lento/.

Méndez, Lucía. "La dopamina de las redes". *Elmundo.es,* 16 de diciembre de 2017. https://www.elmundo.es/opinion/2017/12/16/5a342ccce5fdea97248b4626.html.

Nahabetián Brunet, Laura. "Protección de datos personales *vs*. Acceso a la información pública. ¿Derechos fundamentales en conflicto?". http://www2.congreso.gob.pe/sicr/cendocbib/con2_uibd.nsf/C43D4582907B5890052578080076 3C5A/%24FILE/nahabetian.pdf.

Pérez Tejada, Carlos. "¿Quién hace negocio con tu data personal?". *Diario Libre,* 11 de junio de 2019. https://www.diariolibre.com/estilos/blogs/martes-de-tecnologia/quien-hace-negocio-con-tu-data-personal-EB13034220.

DR © Konrad Adenauer Stiftung e. V. - http://www.kas.de/rspla/es/

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas-colaboracion.juridicas.unam.mx/

Prats, Eduardo Jorge. *Derecho constitucional*, volumen II. Santo Domingo: Ius-Novum, 2016.

Scolnik, Hugo. *Qué es la seguridad informática.* Buenos Aires: Paidós, 2014.

Solares, Rafael. "La nomofobia: la adicción a nuestros celulares". *Forbes México*, 13 de marzo de 2018. https://www.forbes.com.mx/la-nomofobia-la-adiccion-a-nuestros-celulares/.

Subero Isa, Jorge. *Tratado práctico de responsabilidad civil dominicana.* Santo Domingo: Corripio, 2018.

Refojos, María. "Teletrabajo y ocio disparan el consumo de internet: ¿están las redes preparadas para el coronavirus?". *El Periódico*, 19 de marzo de 2020. https://byzness.elperiodico.com/es/innovadores/20200319/coronavirus-teletrabajo-ocio-consumo-internet-preparados-7895752.

Toffler, Alvin y Heidi Toffler. *La revolución de la riqueza.* Ciudad de México: Editorial Random House Mondadori, 2006.

Rodríguez, Namphi. "Gaceta Judicial. Redes sociales, campañas electorales y libertad de expresión: límites constitucionales". *Gacetas Judiciales,* 386, 2019. https://do.vlex.com/vid/redes-sociales-campanas-electorales-839612146?_ga=2.177582373.1850323928.1601907386-275380030.1601907386.

DR © Konrad Adenaur Stiftung e. V. - http://www.kas.de/rspla/es/