DERECHO DE LAS TECNOLOGÍAS
Y LAS TECNOLOGÍAS PARA EL DERECHO

COLECCIÓN
BIBLIOTECA JURÍDICA UNIANDINA

La Colección Biblioteca Jurídica Uniandina se creó en el 2008. Sus publicaciones se destacan por la variedad temática en las áreas de derecho privado, derecho público, derecho penal, derecho internacional, derecho procesal y teoría jurídica. Las obras que acoge son escritas, en su mayoría, por profesores de planta y cátedra de la Facultad de Derecho de la Universidad de los Andes. Estos títulos se emplean, en gran parte, como textos guía en las diferentes asignaturas que componen el pénsum del programa de Derecho de la Facultad.

MARÍA LORENA FLÓREZ ROJAS
(Coordinadora académica)

DERECHO DE LAS TECNOLOGÍAS Y LAS TECNOLOGÍAS PARA EL DERECHO

Grupo de Estudios en Internet, Comercio Electrónico,
Telecomunicaciones e Informática (GECTI)

Universidad de los Andes
Colombia
Facultad de Derecho

Nombre: Flórez Rojas, María Lorena, coordinadora académica, autora. | Cano Martínez, Jeimy José, autor. | Gutiérrez Arboleda, María Paula, autora. | Vicente Blanco, Dámaso-Javier, autor. | Herrera Hincapié, Carolina, autora. |Sandoval Gutiérrez, José Fernando, autor. Guío Español, Catalina, autora.

Título: Derecho de las tecnologías y las tecnologías para el derecho / María Lorena Flórez Rojas (Coordinadora académica) ; Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI).

Descripción: Bogotá : Universidad de los Andes, Facultad de Derecho, Ediciones Uniandes, 2022. | xiv, 212 páginas : ilustraciones ; 16 × 23 cm. | Biblioteca Jurídica Uniandina

Identificadores: ISBN 9789587982954 (rústica) | 9789587982961 (electrónico)

Materias: Tecnología y derecho | Protección de datos | Big Data | Inteligencia artificial |

Clasificación: CDD 344.095-dc23 SBUA

Primera edición: julio del 2022

Ediciones Uniandes
Carrera 1.ª n.° 18A-12, Bloque Tm
Bogotá, D. C., Colombia
Teléfono: 601 3394949, ext. 2133
http://ediciones.uniandes.edu.co
http://ebooks.uniandes.edu.co
infeduni@uniandes.edu.co

ISBN: 978-958-798-295-4
ISBN *e-book*: 978-958-798-296-1
DOI: http://dx.doi.org/10.15425/2017.571

Corrección de estilo: Martha Méndez
Diagramación interior y de cubierta: Andrea Rincón

Impresión:
DGP Editores S. A. S.
Calle 63 n.° 70 D-34
Teléfono: 601 7217641 / 7217756
Bogotá, D. C., Colombia

Impreso en Colombia – *Printed in Colombia*

Universidad de los Andes | Vigilada Mineducación. Reconocimiento como universidad: Decreto 1297 del 30 de mayo de 1964. Reconocimiento de personería jurídica: Resolución 28 del 23 de febrero de 1949, Minjusticia. Acreditación institucional de alta calidad, 10 años: Resolución 582 del 9 de enero del 2015, Mineducación.

Contenido

Capítulo II

El *big data* como tecnología disruptiva en Colombia

Carolina Herrera Hincapié

Capítulo III

Inteligencia artificial en el mercado: presagios sobre la aplicación del régimen de competencia desleal

José Fernando Sandoval Gutiérrez

CAPÍTULO IV

SANDBOXES REGULATORIOS: UN ENFOQUE INNOVADOR PARA LA REGULACIÓN DE LAS *FINTECHS*

CATALINA GUÍO ESPAÑOL

CAPÍTULO V

EL DETERMINISMO ALGORÍTMICO EN COLOMBIA: RIESGOS PARA LA PROTECCIÓN DEL USUARIO

MARÍA LORENA FLÓREZ ROJAS

Presentación

Agradezco sinceramente la invitación a escribir la presentación de este libro por parte de María Lorena Flórez Rojas, directora del Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes. Para cumplir este honroso encargo, resultaba inevitable hacer una retrospectiva de lo que ha sido este grupo de estudios, compuesto por grandes profesionales y amigos, que con su desinteresado aporte a la discusión de temas sensibles del derecho y las tecnologías han contribuido a la producción de importantes investigaciones y discusiones que hoy son de referencia obligada, no solo de los estudiosos del derecho, sino, incluso, en pronunciamientos de nuestras altas corporaciones, y docentes nacionales e internacionales.

Este libro con el que hoy celebramos el vigésimo aniversario del GECTI no es producto aislado de una iniciativa dirigida simplemente a esta conmemoración, sino que es fruto del esfuerzo continuado de sus miembros por compartir y discutir temas trascendentales en este mundo tan dinámico del derecho, a partir del desarrollo de tecnologías disruptivas que hoy nos plantean grandes retos.

En efecto, este grupo de estudios que buscaba concitar una labor colectiva y armónica por generar y difundir conocimiento en temas de tecnología llega este año a su vigésimo aniversario, cuando de la mano de su anterior director y fundador, el profesor Nelson Remolina Angarita, se echó a andar un proyecto que, como muchos de los grandes proyectos, no fue ni planeado ni desarrollado al detalle para su iniciación. Tal como lo conversábamos con el profesor Remolina rememorando lo que han sido estos veinte años, simplemente el mundo empezó a hablar en esas calendas, y aún antes, de temas de tecnología y derecho, sin que infortunadamente países como Colombia pudieran acceder con facilidad a literatura sobre la materia, a menos que fuera en inglés. A partir de esa realidad nació el GECTI.

De allí que esta idea ha sido desarrollada por la generosa y desinteresada contribución de un grupo de profesionales expertos en sus áreas, que le dieron vida y continuidad a esta iniciativa que hoy tiene en su caudal innumerables publicaciones, congresos y seminarios, cursos de educación continua y, por supuesto, presencia a nivel internacional de miembros del grupo en actividades académicas en otras universidades e instituciones de gran relevancia.

Hoy recordamos cómo en el 2002, de la mano de Legis, publicábamos temas de desmaterialización del documento electrónico, *habeas data*, evidencia digital, comercio electrónico e internet, modelos de negocios y contratos en internet, aspectos tributarios del comercio electrónico, la propiedad intelectual en el entorno digital, temas de jurisdicción y competencia en materia de conflictos nacidos en internet, protección de las bases de datos electrónicas, nombres de dominio, entre otros temas. Y en el 2003, también con Legis, tratábamos temas de gobierno electrónico, ciberdelincuencia, soberanía estatal en internet, videovigilancia, televisión por satélite y, en fin, otros tantos estudios juiciosos sobre temas de gran relevancia en el mundo del derecho y la tecnología en su momento y hoy en día.

En esta oportunidad, tengo el placer de presentar esta publicación, que —como lo decía al inicio— es producto de la contribución de un grupo de profesionales que ha logrado darle continuidad a esta gesta colectiva, desarrollando importantes investigaciones que hoy son de gran relevancia a nivel global. Esta obra resulta de gran trascendencia pues fue escrita durante un año lleno de retos personales para todos los autores, teniendo en cuenta la situación global actual. Sin embargo, este esfuerzo demuestra que ellos no solo se enfocan en presentar los avances en sus materias de investigación, sino que también buscan proponer aspectos innovadores en la educación, la regulación y las buenas prácticas.

Encontraremos temas como el que nos presentan Jeimy J. Cano M., Paula Gutiérrez Arboleda y Dámaso Javier Vicente Blanco, quienes abordan las nuevas cibercompetencias de que deben disponer los profesionales del derecho, así como los jueces y legisladores. Tal como lo manifiestan los autores, hoy más que nunca resulta inconcebible el ejercicio de la profesión sin el tratamiento de datos personales y lo que ello conlleva por virtud del desarrollo tecnológico, motivo por el cual se aborda no solo el estado actual y los retos que se presentan, sino también propuestas concretas que contribuyen a producir los cambios que

se requieren para tratar con propiedad aspectos de la seguridad de la información y protección de datos personales.

Carolina Herrera Hincapié, por su parte, aborda el tema del *big data* como tecnología disruptiva en Colombia e invita a reflexionar sobre el papel de tecnologías de la información como el *big data* en el día a día de las personas, para concientizarlas sobre sus beneficios y riesgos, y los derechos de los cuales son beneficiarios como titulares de los datos, entendidos estos últimos como la materia prima para el correcto funcionamiento de este tipo de tecnologías y su constante mejora.

El flujo masivo de información nos invita a analizar los beneficios y riesgos derivados de su explotación. Por este motivo, el presente artículo además de abordar el estado actual de la regulación en Colombia, propone un conjunto de prácticas y códigos de conducta que les permitan a los titulares de la información una sana explotación de sus datos.

Por su parte, José Fernando Sandoval Gutiérrez trata un tema inevitable en estas discusiones y es el atinente a la inteligencia artificial (IA), esta vez enfocada en los mercados y el régimen de competencia. La incursión de la inteligencia artificial en todos los ámbitos de la vida es innegable; por ello, sus implicaciones en las normas existentes en materia de competencia obligan a discernir sobre el futuro de tales normas y su aplicación frente a comportamientos en el mercado que pueden o no resultar desleales a partir del uso de esta tecnología.

Los servicios financieros tampoco han sido ajenos a la evolución tecnológica, de allí que Catalina Guío Español nos presente un interesante estudio relativo a estas nuevas tecnologías financieras y modelos de negocios, que si bien buscan la innovación y la competitividad, deben adelantarse bajo parámetros que logren la estabilidad financiera, pero también la protección a los consumidores. El análisis de lo que se ha hecho a nivel internacional frente a los *sandboxes* regulatorios resulta ser una figura exitosa en varios países, que sin duda deberá tenerse en cuenta en el futuro próximo, como una forma de abordar los desafíos planteados por las *Fintechs*.

Finalmente, nuestra directora, María Lorena Flórez Rojas, examina un tema de absoluta relevancia en la actual sociedad de consumo, considerando que el consumidor actual ha venido desarrollando comportamientos diversos frente a las tecnologías, donde los algoritmos muchas veces han influenciado, o no, la decisión de consumo. A lo largo de este

capítulo se analiza el comportamiento del consumidor con relación a la intervención tecnológica de los algoritmos en los procesos de compra en línea y cómo la inteligencia artificial, combinada con procesos de consumo, puede llegar a afectar las decisiones de los mismos consumidores, ya sea de manera consciente o inconsciente. Las ventajas de la IA son innegables, pero los inconvenientes que produce no pueden dejarse de lado, y su análisis debe darse sin duda alguna para evitar, entre otras, la vulneración de derechos de los consumidores y las afectaciones propias de la alteración en la capacidad de decisión en la adquisición de productos y/o servicios. Si a eso le sumamos el aumento vertiginoso del comercio electrónico, el tema resulta ser más sensible; aspectos como el suministro de información previa y clara, la calidad y garantía de los productos y servicios, la protección adecuada de la información del consumidor y la seguridad en los medios de pago obligan a analizar en profundidad el tema para la adecuada y eficaz protección al consumidor.

En consecuencia, hoy, como hace veinte años, en el GECTI continuamos discutiendo temas que nos retan en cuanto a su análisis y solución, y en los cuales el ejercicio del derecho nos obliga a ser dinámicos frente a realidades tecnológicas que ya son parte de nuestra cotidianeidad.

Felipe Rubio Torres
Miembro del GECTI

Capítulo I

La imposición de cibercompetencias en el ejercicio de la abogacía por cuenta de la protección de datos personales*

Jeimy J. Cano M.
Paula Gutiérrez Arboleda
Dámaso Javier Vicente Blanco

Introducción

Es inconcebible el ejercicio de la abogacía sin el tratamiento de datos personales. Esto conlleva obligaciones legales y deontológicas. El mero hecho de ser indispensable para resolver un proceso judicial no faculta a los abogados implicados a decidir cómo recogerlos, conservarlos, compartirlos, transmitirlos, modificarlos o eliminarlos sin tener en cuenta los riesgos en materia de seguridad. Además, siempre que se contemplen datos personales la información debe ser manejada bajo los principios de *accountability*, licitud del tratamiento, lealtad, transparencia, exactitud, minimización, integridad y confidencialidad. Todos ellos priman en el nuevo orden jurídico-digital internacional, y no solo aplican para las empresas privadas u organizaciones del sector público, sino muy específicamente para los abogados desde la doble vertiente de sus obligaciones legales y deontológicas. Como cualquier profesional, los de la rama del derecho han visto transformarse dramáticamente su *modus operandi* en los últimos diez años por efecto de la digitalización y el desarrollo tecnológico, con el agravante de que en su caso tiene unas consecuencias que van más allá de la competitividad económica o la eficiencia productiva, puesto que repercuten legalmente en la vida de las personas y en el

* Para citar este capítulo: http://dx.doi.org/10.15425/2017.572.

marco en que se desenvuelven todas las relaciones de un país, otorgando condiciones de estabilidad y garantías para el desarrollo.

Todas las obligaciones que se desprenden de este entramado legal afectan como empresas a los despachos de abogados. A su vez, todas las garantías que son exigibles determinan cambios en materia procesal y conllevan la asunción de medidas técnicas, organizativas y formativas, no solo para los especialistas en *Legaltech*, sino para todas las áreas del derecho.

Este capítulo aborda las medidas que resultan exigibles en materia de seguridad de la información y protección de datos personales a todos ellos, desde un abogado que trabaja de forma independiente, hasta una gran firma legal, a la vez que analiza las principales implicaciones de este derecho fundamental en los procesos jurídicos, intentando proponer unos estándares mínimos en materia de ciberseguridad, gestión de riesgos y comprensión de las nuevas tecnologías.

El Reglamento General de Protección de Datos de la Unión Europea impone nuevos estándares de privacidad en el mundo

El flujo masivo de datos personales en internet ha aumentado exponencialmente la cantidad y gravedad de riesgos y amenazas a la dignidad humana en las últimas décadas, lo que ha obligado a trabajar en defensa de los derechos individuales y a evitar la trivialización de dichos riesgos. Las respuestas constitucionales y normativas internacionales con fuerza de ley son ineludibles en el globo terráqueo. Internet es el gran instrumento contemporáneo del que la sociedad se sirve para ampliar sus capacidades de información y conocimiento, pero son necesarios nuevos derechos para asegurar que tratamientos no autorizados o directamente corruptos pongan en juego la libertad, dignidad y seguridad de la raza humana y de cada uno de sus componentes[1].

Durante muchos años existió un desfase temporal entre la regulación y la innovación tecnológica, que dejaba al criterio de los juristas la forma de actuar frente a temas para muchos de ellos desconocidos. No obstante, un entramado de normas entre las que se destacan el

[1] Artemi Rallo, "Privacy and Freedom", *European Data Protection Law Review* 4, n.º 2 (5 de febrero del 2018): 150-51. https://edpl.lexxion.eu/article/EDPL/2018/2/5.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril del 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos [RGPD])[2], la Ley Orgánica 3/2018, de 5 de diciembre del 2016, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)[3] (española), la directiva *ePrivacy* y su propuesta de reglamento, la Directiva 2016/680 de protección de datos personales en el proceso penal, la Directiva NIS[4], el Reglamento General de Ciberseguridad, el Reglamento General de Protección de Datos No Personales, o la Ley de Secretos Empresariales (española), llegó para quedarse y ha dado un vuelco a la profesión del abogado, juez o notario como responsable y como encargado del tratamiento.

Este entramado legal, originado fundamentalmente en Europa, y que en principio solo afecta a los residentes europeos y a organizaciones y empresas que interactúen con ellos (aunque estén en Latinoamérica, Canadá, Oceanía o cualquier punto del globo), ha traído consigo la "consolidación de nuevos derechos y posibilidades, que a su vez provocarán una mejor circulación de datos, un aumento de la seguridad jurídica, nuevos métodos de resolución de problemas, y una regulación armonizada directamente vinculante"[5, 6].

[2] Reglamento General de Protección de Datos (RGPD), Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril del 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). *DOUE* 119, 4 de mayo del 2016.

[3] Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), Ley Orgánica 3/2018, de 5 de diciembre del 2016, de Protección de Datos Personales y Garantía de los Derechos Digitales. *Boletín Oficial del Estado* 294, Sec. I, p. 119791 (2018).

[4] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio del 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

[5] Alfonso Ortega Jiménez y Juan José Gonzalo Domenech, "Nuevo marco jurídico en materia de protección de datos de carácter personal de la Unión Europea", *Revista de la Facultad de Derecho. Universidad de la República de Uruguay*, n.º 44 (2018): 93.

[6] Algunos autores cuestionan, sin embargo, la ansiada uniformidad legislativa europea por las numerosas oportunidades en que se deja a criterio de los Estados la

Todo ello se ha materializado en la redefinición de políticas de privacidad en todo el mundo, una revisión de las medidas de seguridad exigibles para datos personales básicos y sensibles y un rediseño de procesos con la privacidad por defecto en todos los sectores de actividad y, por supuesto, en el legal. En el primer año desde la entrada en vigor del RGPD surgieron nuevas políticas de protección de datos y/o ciberseguridad en Perú, Brasil, Chile, Uruguay e incluso territorios al otro lado del mundo, como Israel y Hong Kong[7]. En el 2021 surgió el Reglamento de Protección de Datos en Ecuador.

La puesta en marcha no ha sido fácil. Una encuesta realizada por Thomson Reuters en diciembre del 2017 y repetida en diciembre del 2018 en empresas de nueve países con un promedio de ingresos de 282 millones de dólares (en todo el mundo) y de 16 400 empleados reveló que cumplir con el RGPD es tan difícil o más de lo que esperaban (66 %); en consecuencia, la mitad acepta que no solo les consume gran parte de sus presupuestos para proteger la privacidad, sino que estos debían crecer hacia el futuro[8]. El 91 % se consideran conocedores del RGPD, pero apenas el 76 % reporta una comprensión más completa de las implicaciones de sus 99 artículos[9], sin que necesariamente los estén abordando todos (de hecho, la mitad reconoce el riesgo de quedarse atrás en su aplicación).

Desde la implementación del RGPD, las empresas se están volviendo menos proactivas en sus políticas de captación de consumidores por motivos relacionados con la privacidad. Se destaca el caso de Estados Unidos, en donde un año atrás el 60 % de las empresas reportaba

---

adaptación y garantía de aplicación normativa del RGPD (más de medio centenar) y por la abundancia de conceptos jurídicos indeterminados incluidos en él, tales como "lo que sea necesario" o que "resulte adecuado", "oportuno" o "necesario", a los que se recurre en más de doscientas oportunidades a lo largo del reglamento. Véase: Ana Isabel Herrán Ortiz, "Aproximación al derecho de protección de datos en Europa: El RGPD a debate", *Derecho, Empresa y Sociedad,* n.º 8 (2016): 199 y Rosario García Mahamut, "El derecho fundamental a la protección de datos: El Reglamento 2016/679 como elemento definidor del contenido esencial del artículo 18,4 de la Constitución", *Anuario de Derecho Parlamentario*, n.º extra 31 (2018): 72-73.

[7] "GDPR+1 Year: Business Struggles With Data Privacy Regulations Increasing", *Thomson Reuters*, acceso el 24 de octubre del 2019, http://ask.legalsolutions.thomsonreuters.info/GDPR1YearBusinessStrugglesReport.

[8] *Ibid*.

[9] *Ibid*., 5.

estrategias abiertamente diseñadas para captar consumidores, y a finales del 2018 únicamente lo hacía un 27 %. En términos globales la reducción fue menos drástica, al pasar del 42 % al 30 %. Las compañías estadounidenses encuestadas no solo se tornan más prudentes en sus estrategias de *marketing*, sino que más de la mitad (56 %) da por hecho que afrontará costos crecientes del *compliance* en privacidad para los años venideros, frente al 48 % global[10]. Además, a finales del 2018, el 61 % de las empresas consultadas aceptó que no disponía de las herramientas adecuadas para realizar el seguimiento a las regulaciones y obligaciones de participación de los consumidores que están surgiendo en diversas jurisdicciones geográficas[11].

En Estados Unidos, este efecto dominó legislativo mundial en materia de privacidad y protección de datos ha dado origen a la *Ley de Protección al Consumidor de California (CCPA)*, aplicable a partir del 1.º de enero del 2020, que a su vez ha inspirado otras en diez estados que están formulando sus propias normativas. La CCPA concede a los consumidores nuevos derechos sobre los datos personales. El segundo estado en conseguirlo ha sido Virginia. Su *Ley de Protección de Datos de los Consumidores de Virginia (CDPA)* se sancionó el 2 de marzo del 2021 y entrará en vigor en el 2023. Se espera que Colorado se convierta en el tercer estado de este país en aprobar una ley de privacidad integral. Cabe destacar que en Utah la Ley de Defensa Afirmativa de Ciberseguridad se sancionó el 11 de marzo del 2021 y que Washington, Oklahoma, Vermont y Nueva York, entre otros, han desarrollado propuestas de leyes de privacidad que aún no han logrado superar todas las instancias requeridas[12]. La multiplicidad de leyes en torno a la privacidad y protección de datos, cuyas definiciones y exigencias no siempre coinciden, ha llevado a las todopoderosas multinacionales que más se opusieron a la entrada en vigor del RGPD (como Google, Apple o Facebook) a solicitar una ley federal de protección de datos en Estados Unidos, que marque unas pautas claras por cumplir en toda la nación e impidan

[10] *Ibid*., 7.

[11] *Ibid*., 14.

[12] Christopher J. Buontempo y Cynthia Larose, "US State Privacy Law Check-In-Update", Mintz, https://www.mintz.com/insights-center/viewpoints/2826/2021-04-30-us-state-privacy-law-check-update.

que cada estado imponga sus propias reglas de juego con normativas en algunos casos ambiguas y muy difíciles de cumplir[13]. Y aquí es donde un reciente análisis de *The Economist* apunta, muy acertadamente, que ante la dificultad de competir en materia de inteligencia artificial con Estados Unidos y China, el papel regulador de la Unión Europea es crucial como garante de la protección de datos personales y otros derechos fundamentales en todo el mundo[14].

¿Cómo afecta esto a un abogado en Colombia? En un mundo interconectado, esta incesante aparición de normas en el mundo incrementa los costes de acceso de empresas y profesionales a nuevos mercados y eleva la incertidumbre jurídica. Por un lado, la situación de Silicon Valley en California concentra gran parte del desarrollo tecnológico de aplicaciones, gestores de bases de datos, comunicaciones, buscadores y dispositivos del mundo: Google, Apple, Yahoo, eBay, Adobe, Hewlett Packard (HP), Intel, Cisco, Oracle y Symantec. De manera similar, grandes empresas de ciberseguridad, industria TI, medios de comunicación y servicios en la nube, como Microsoft, Facebook y Amazon Web Services, están ubicadas en Virginia. Como consumidor, es prácticamente impensable que un abogado en Colombia, Estados Unidos o la Unión Europea ejerza sus funciones al margen de todos estos productos, aunque algunos no sean bien vistos a los ojos de las autoridades de protección de datos. Como profesional, el abogado que ejerza como *compliance officer* o *data protection officer* de una empresa cuyos clientes estén fuera de Colombia deberá conocer la legislación que se debe cumplir en cada uno de sus mercados de destino; en el caso de Estados Unidos, al regirse por normas de protección de datos diferentes según el estado, deberá aplicar la de cada estado al que quiera dirigirse.

Por ello, los analistas consideran necesario "establecer estándares universales de protección de datos, que permitan flujos internacionales

[13] Alejandro Padín Vidal, "Protección de datos en Colombia, Perú, México y Brasil: referencia a Estados Unidos", en *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, editado por José López Calvo *et al*. (Hospitalet de Llobregat: Bosch Wolters Kluwer, 2019), 1057-1084.

[14] "Big Data, Small Politics: Can the EU Become Another AI Superpower?", *The Economist*, 20 de septiembre del 2018, 12-13.

de información con garantías efectivas, estableciendo un modelo uniforme a estos efectos a nivel europeo e internacional"[15].

A pesar de la multiplicidad de legislaciones en protección de datos, los ciberriesgos para los despachos de abogados son globales, si bien, en muchos casos, los objetivos no son en sí mismos los profesionales del derecho, sino sus clientes. En el cuadro I.1 se recogen algunos de los mayores ciberataques padecidos por firmas de abogados alrededor del mundo y sus consecuencias. Estos ejemplos muestran que las firmas de abogados pueden ser objeto de los ciberdelincuentes con distintos fines: lucrativo (en el caso de Toronto), reputacional del propio despacho o sus profesionales, ideológico o político. Por medio de los abogados, los atacantes logran acceder en ocasiones a información privilegiada de sus clientes (como en los casos de Londres y Washington), o de altos cargos de gobiernos que pueden desestabilizar una o varias naciones a la vez (como en el caso de los papeles de Panamá). Otras veces van detrás de planes estratégicos, información financiera u otros secretos empresariales de grandes industrias (Nueva York), incluidos datos personales, que por el mero hecho de ser publicados o utilizados por terceros pueden beneficiar directamente a los atacantes o a competidores dispuestos a pagar por esa información.

Aquí entra en juego la necesidad de preservar legalmente la dignidad de las personas, introduciendo con el RGPD un cambio de paradigma. Tradicionalmente, las visiones de la privacidad de Estados Unidos y Europa han estado enfrentadas, puesto que, mientras que en la Unión Europea la protección de datos personales es un derecho fundamental con todas las garantías, en Estados Unidos se ha entendido durante décadas como un servicio de pago. Allí, algunas de las normas estatales vigentes buscan remedios posteriores a la violación de datos, en lugar de centrarse en medidas preventivas. Si el espíritu de la norma es esperar a que una empresa o despacho sea hackeado, antes de determinar que sus medidas de protección eran inadecuadas, seguirán estando desprotegidas la información de los clientes, la reputación del despacho y su continuidad en el negocio (al estar expuesto a tener que reparar a las

[15] Mónica Martínez López-Sáez, "Una reflexión del derecho fundamental a la protección de datos de carácter personal" (Valencia: Tirant Lo Blanch, 2018).

Cuadro I.1. Principales ataques contra firmas de abogados en el mundo

Firma	Lugar	Consecuencias	Año
Jones Day	Estados Unidos	Revelación de secretos en la web oscura de clientes como Donald Trump, Optus y Singtel (telecomunicaciones) y chantaje al despacho.	2021
Grubman Shire Meiselas & Sacks	Estados Unidos	Revelación de secretos en la web oscura de clientes como Robert de Niro, Lady Gaga, Madonna, Rod Stewart, U2, Mike Tyson, Lebron James y Mariah Carey, y chantaje al despacho.	2020
DLA Piper	Reino Unido	Atacado por un *ransomware* que paralizó la firma varios días; les pedían unos 300 dólares en bitcoines a modo de rescate.	2017
Mossak Fonseca	Panamá	Más de 11,5 millones de documentos publicados (más de 2,6 TB de datos). Reveló el mayor fraude fiscal conocido, con consecuencias en todo el mundo; se vieron afectados ciento cuarenta altos dirigentes políticos y personalidades públicas de cincuenta países diferentes que participan o han participado en sociedades *offshore*, entre ellos doce jefes y exjefes de Estado.	2016
Cravath, Swaine & Moore y Weil Gotshal & Manges	Estados Unidos	Intercambio de información privilegiada que incluía fusiones planificadas, lo que permitió a sus usuarios ganar más de cuatro millones de dólares.	2016
48 grandes bufetes	Estados Unidos y Reino Unido	46 bufetes en Estados Unidos y dos en el Reino Unido fueron alertados de ataques desde Ucrania por parte del *hacker* Oleras, que ofrecía servicios de *phishing* en su contra en un sitio web ruso. Según el *Wall Street Journal*, esto estaba relacionado con las infracciones de marzo del 2016 contra los principales bufetes de abogados.	2016

39 Essex Street	Reino Unido	39 Essex Street fue atacada cibernéticamente. Booz Allen Hamilton, empresa consultora de tecnología, informó que el ataque muy probablemente provino del grupo ruso Oso Energético, patrocinado por el Estado. Este grupo estuvo vinculado a la piratería de empresas de servicios públicos en Estados Unidos y Europa en el 2014.	2014
Bufete canadiense	Canadá	Un bufete fue atacado por un virus informático que robó una cantidad de seis cifras de su cuenta fiduciaria. Los *hackers* instalaron un virus troyano para acceder a las contraseñas de las cuentas bancarias de la empresa.	2012
Wiley Rein	Estados Unidos	Wiley Rein, uno de los bufetes de abogados más grandes de Washington, D. C., fue hackeado, al parecer, por agentes chinos patrocinados por el Estado. Según Bloomberg News, los *hackers* querían información relacionada con SolarWorld, el fabricante alemán que produce paneles solares, cuyos sistemas fueron pirateados casi al mismo tiempo.	2012

Fuentes: Debra Cassens Weiss, "Jones Day Is Hit by Vendor Data Breach; Hackers Post Files They Claim Were Stolen from the Law Firm", 17 de febrero del 2021, https://www.abajournal.com/news/article/jones-day-is-hit-by-vendor-data-breach-hackers-post-files-they-claim-were-stolen-from-the-law-firm. Joe Tidy, "Hackers Hit A-List Law Firm of Lady Gaga, Drake and Madonna", *BBC News*, 12 de mayo del 2020. Julie Sobowale, "Six Major Law Firm Hacks in Recent History", *ABA Journal* (marzo del 2017). "Los principales líderes políticos de 'Los Papeles de Panamá'", *ElDiario.es*, 3 de abril del 2016, https://www.eldiario.es/economia/politicos-mundiales-aparecen-Papeles-Panama_0_501500208.html.

Nota: La American Bar Association (ABA) es el equivalente al Colegio de Abogados de Estados Unidos, del que son miembros voluntarios 410 000 profesionales del derecho.

partes perjudicadas o afrontar cuantiosas sanciones monetarias)[16]. Eso es lo revolucionario de la CCPA y de las demás leyes que se están creando en otros estados, máxime cuando la situación en Estados Unidos llegó al punto de que, en marzo del 2017, cuando el RGPD ya se había publicado y estaba en periodo de carencia, los republicanos aprobaron en el Congreso una ley que daba carta blanca a los proveedores de internet para almacenar y vender los datos de los usuarios sin su consentimiento[17].

En esta lucha de poder que enfrenta los intereses economicistas con los derechos fundamentales, la Unión Europea nunca ha estado en condiciones de imponer reglas fuera de su territorio. Sin embargo, el tamaño del mercado europeo es suficientemente grande para no ser despreciado por ninguna de las multinacionales de Silicon Valley ni por otras, como Facebook o Huawei (que hasta la entrada en vigor de esta legislación podían salir indemnes después de vulnerar los derechos de los residentes europeos, pues, a pesar de haber fallos en su contra, al no estar obligadas a tener sede fiscal ni responsable legal en Europa, los afectados tenían que enfrentar pleitos contra ellas en sus países de origen, con los inasumibles costes que ello suponía). Las autoridades de la Unión Europea supieron aprovechar esta situación forzando un vuelco mundial al exigir que todos los actores que quisieran mantener sus operaciones con ciudadanos residentes en Europa se vieran obligados a fijar un responsable legal en territorio europeo y cumplir, como cualquier empresa europea, el riguroso RGPD. Como ninguna gran multinacional tecnológica quería quedarse sin el trozo europeo del pastel, las empresas estadounidenses tuvieron que adherirse al Privacy Shield (Escudo de Privacidad para las transferencias internacionales de datos desde la Unión Europea hacia Estados Unidos) y comprometerse a sumarse a las empresas cumplidoras, a pesar de no estar obligadas por sus legislaciones de origen. En este sentido,

[16] Madelyn Tarr, "Law Firm Cybersecurity: The State of Preventative and Remedial Regulation Governing Data Breaches in The Legal Profession", *Duke Law & Technology Review* 15, n.º 1 (2016): 251.

[17] Cecilia Kang, "Congress Moves to Overturn Obama-Era Online Privacy Rules", *The New York Times*, 28 de marzo del 2017, https://www.nytimes.com/2017/03/28/technology/congress-votes-to-overturn-obama-era-online-privacy-rules.html?smid=tw-nytimes&smtyp=cur.

> […] el Parlamento Europeo tuvo en cuenta la jurisprudencia del Tribunal de Justicia en una materia tan sensible para la representación electiva de la ciudadanía como es la que concierne al nivel de protección del que gozan los ciudadanos europeos ante las empresas y autoridades estadounidenses. Así ha sido el caso, en todo lo relativo al acceso equitativo a recursos administrativos y jurisdiccionales ante eventuales lesiones de su privacidad en la masiva transmisión electrónica de datos personales que ha experimentado el impacto de la revolución tecnológica e informacional, en un momento de la historia en que la seguridad ha emergido como nunca como prioridad política —en consecuencia al flagelo del crimen organizado, el terrorismo global y la "radicalización" de la amenaza yihadista—, con una fuerza de choque sobre nuestros ordenamientos (y sobre el frágil equilibrio "libertad/seguridad") inédita hasta el tiempo presente[18].

Pero las garantías ofrecidas por este escudo no resultaron suficientes para todos. En julio del 2020, el Tribunal de Justicia de la Unión Europea invalidó el Privacy Shield motivado en que la normativa interna estadounidense relativa al acceso y la utilización de los datos transferidos desde la Unión Europea, por parte de sus autoridades, no se rige por el principio de proporcionalidad, cuando de medidas de vigilancia masiva se trata, ni tampoco confiere a los interesados derechos exigibles a las autoridades estadounidenses ante los tribunales[19].

Este capítulo toma como estándar de cumplimiento el RGPD por haber sido la punta de lanza para la regulación de la privacidad, que ya se ha materializado y se va a seguir imponiendo en muchos países, para devolver a los ciudadanos los derechos sobre su información personal y obligar —bajo el principio de *accountability* y desde la perspectiva del análisis de riesgos— a empresas, gobiernos y organizaciones de todo el mundo a implementar altos estándares técnicos, organizativos,

[18] Juan Fernando López Aguilar, "La protección de datos personales en la más reciente jurisprudencia del TJUE: Los derechos de la CDFUE como parámetro de validez del derecho europeo y su impacto en la relación trasatlántica UE-EEUU", *Teoría y Realidad Constitucional*, n.º 39 (2017): 580.

[19] Tribunal de Justicia de la UE (Gran Sala) Sentencia de 16 de julio del 2020, Asunto C-311/18. Data Protection Commissioner contra Facebook Ireland Ltd. y Maximillian Schrems.

contractuales y formativos en materia de seguridad de la información y derechos de los titulares de los datos. Muchas multinacionales ya ponen en sus políticas de privacidad el RGPD como su modelo y pretenden cumplirlo a escala mundial[20].

> Las facultades de control del RGPD refuerzan la posición jurídica de los interesados con la introducción del derecho al olvido y la consolidación de los derechos de rectificación, oposición y limitación del tratamiento… no obstante, en el éxito o fracaso del sistema de garantías del RGPD, el responsable del tratamiento juega un papel determinante, como lo hará, en caso de ser designado voluntariamente o por obligación, el delegado de protección de datos, que en calidad de mediador puede contribuir a ponderar los intereses del titular de los datos con los del responsable del tratamiento[21].

Lo anterior podría llegar a evitar incluso la intervención de la autoridad de control. Además, la introducción del

> [...] Derecho a la Portabilidad, en cuanto manifestación del derecho a la autodeterminación informativa, puede ser de gran utilidad en la consecución de un espacio de libre circulación de datos mejor conectado, especialmente en materias como la asistencia sanitaria transfronteriza o la investigación biomédica, al facilitar la transmisión de datos de salud y genéticos, que el interesado haya consentido tratar y transferir[22].

Es de esperar que una sociedad tan garantista en materia legal como la colombiana, cuya legislación en cuanto a protección de datos personales (Ley 1581 del 2012 y Decreto 1377 del 2013) se inspiró en la Directiva 46/1995 de la Comisión Europea[23], establezca a corto plazo

[20] Padín Vidal, "Protección de datos", 1084.

[21] Daniel Jove Villares, "Las facultades de control de la información personal en el RGPD", en *Derecho, gobernanza e innovación: Dilemas jurídicos de la contemporaneidad en perspectiva transdisciplinar,* coordinado por Maria Manuela Magalhães, Rubén Miranda Gonçalves y Fábio da Silva Veiga (Universidade Complutense: 2017), 377-378.

[22] *Ibid*.

[23] Padín Vidal, "Protección de datos", 1057-1061.

modificaciones en el nuevo reglamento, pues si bien incorpora como el RGPD el principio de *accountability* y la posibilidad de hacer transferencias internacionales de datos supeditada al cumplimiento de una serie de garantías, resulta insuficiente para asegurar las medidas exigibles para proteger los datos de carácter personal frente a los últimos desarrollos tecnológicos y su rápida evolución, los derechos digitales de los ciudadanos en general y los trabajadores en particular, el derecho al acceso universal a internet y su principio de neutralidad. También es muy importante el papel que desempeñan los delegados de protección de datos en el cumplimiento del RGPD y la LOPDGDD en las empresas y organizaciones privadas con riesgos específicos y de todos los entes del sector público. A nuestro entender, hace falta equiparar de manera más formal la figura del oficial de protección de datos contemplada en la *Guía para la implementación del principio de responsabilidad demostrada* de la Superintendencia de Industria y Comercio[24] con la del delegado de protección de datos del RGPD, y crear un esquema de certificación que profesionalice este perfil, así como introducir otras novedades legales (entre otras, derecho de portabilidad, obligación de reportar brechas de seguridad con consecuencias para los derechos y libertades de las personas en un plazo perentorio a la autoridad de protección de datos, y nuevas categorías de datos personales[25]) para que Colombia cuente con estándares similares a los europeos y pueda ser incluida en el listado de destinatarios declarados de nivel adecuado para transferencias internacionales de datos personales por la Comisión Europea[26], por el impacto que esto tiene en el comercio bilateral (UE-Colombia). Además, esto podría tener repercusión positiva en las relaciones entre Colombia y otros países en los ámbitos comercial, turístico, de defensa de derechos

[24] Superintendencia de Industria y Comercio, *Guía para la implementación del principio de responsabilidad demostrada* (Bogotá, 2017), 10-12, https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf.

[25] "Cumplimiento de las obligaciones", Agencia Española de Protección de Datos, acceso el 28 de mayo del 2021, https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes.

[26] Este listado se puede consultar en la página web de la Agencia de Protección de Datos, en el apartado de transferencias internacionales. Al día de hoy, el único país latinoamericano que a juicio de la Comisión Europea presenta las garantías adecuadas es Argentina. Véase https://www.aepd.es/reglamento/cumplimiento/transferencias-internacionales.html.

fundamentales, atracción de inversión extranjera directa y de cooperación internacional.

En materia de garantía de los derechos digitales se toma como referencia la LOPDGDD española[27], por ser la primera que, tras actualizar la normativa nacional en cumplimiento del RGPD[28], vincula la protección de datos personales con los derechos digitales de los usuarios. Estos últimos incluyen el derecho a la neutralidad de internet, al acceso universal a internet, a la seguridad digital, a la educación digital, a la protección de los menores en internet, a la rectificación en internet, a la actualización de informaciones en medios de comunicación digitales, a la intimidad y al uso de dispositivos digitales en el ámbito laboral, a la desconexión digital en el ámbito laboral, a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral, al olvido en búsquedas de internet y en servicios de redes sociales, a la portabilidad en servicios de redes sociales y al testamento digital[29]. Sin duda alguna, el ejercicio de los derechos digitales parte de la capacidad de los ciudadanos de entender los riesgos a los que se exponen por el uso de medios digitales en las distintas facetas de su vida y los propios derechos que en este sentido les están legalmente garantizados, por lo que la nueva formación en el uso y la seguridad de medios digitales en el sistema educativo español es todo un acierto[30].

[27] Ley Orgánica 3/2018, de 5 de diciembre del 2018, arts. 79-97.

[28] El RGPD no requiere transposición, por ser de obligado cumplimiento para todos los Estados miembro, pero da potestad para que cada uno de ellos adopte decisiones sobre puntos específicos de la norma, como la edad desde la que un menor puede prestar consentimiento expreso e informado sobre el uso de sus datos personales, o el listado de actividades del tratamiento en las que resulta exigible la evaluación de impacto en protección de datos, por citar solo dos ejemplos.

[29] La LOPDGDD ha recibido numerosas críticas "desde el punto de vista de técnica legislativa por el uso excesivo de disposiciones adicionales y finales para introducir cambios de profundo calado social […] y desde el punto de vista sistemático por incluir los derechos digitales dentro de la norma que regula la protección de datos personales, considerando que, por su importancia y entidad, podrían haberse regulado de forma independiente". Roberto Mayor Gómez, "Principales novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales". *Gabilez*, n.º 16 (diciembre del 2018): 54.

[30] *Ibid*., 55.

Más adelante abordaremos la necesidad de ir más allá creando planes de concienciación y formación en ciberseguridad y protección de datos, específicos para los profesionales del derecho.

Conductas inseguras y sus consecuencias

Podemos considerar una debilidad del despacho de abogados frente a sus clientes, sus empleados, las autoridades y la propia competencia cualquier medida técnica, organizativa o formativa que debía haber implementado para asegurar la confidencialidad, disponibilidad e integridad de los datos personales y la información sensible de cuyo tratamiento es responsable o encargado, pero no lo ha hecho, o lo ha hecho deficientemente.

Algunas de estas medidas estaban contempladas en normativas anteriores. Por ejemplo, en España, los abogados, en el ejercicio de su profesión, están obligados a cifrar el fichero de clientes en razón de los artículos 18 y 24 de la Constitución española y del artículo 5 del Código Deontológico español[31] (más adelante haremos un paralelismo con la normativa Colombia). Más recientemente, "el art. 104 del Reglamento 1720/2008 nos obligó a cifrar los mensajes por *e-mail* referidos a resoluciones judiciales"[32] y otras informaciones sensibles de los interesados… pero no siempre se cumplía porque "enviar mensajes en abierto es mucho más cómodo para el que los manda y también para el que los recibe"[33].

El planteamiento ahora es diferente: en el caso que nos interesa, el abogado será el responsable, quien decidirá si manda correos electrónicos o no, si lo hará cifrándolos, o no. Deberá hacer un análisis de la situación, estudiar el estado de la ciencia (pidiendo informes a peritos informáticos), el riesgo (probabilidad y gravedad), el contenido y el contexto. Leerá el RGPD, concretamente el artículo 32.1.a. Dejará los criterios y las conclusiones de esta reflexión por escrito en un registro

[31] Abanlex, *Primer informe sobre la obligación legal de cifrar información y datos personales* (Madrid: Sophos, 2014), 4.

[32] Ignacio Subiza Pérez, "Sobre cómo nos hemos hecho adultos, casi sin darnos cuenta: Nuevo Reglamento Europeo de Protección de Datos", *Actualidad Administrativa*, n.os 7-8 (2018): 3.

[33] *Ibid*.

de las actividades del tratamiento (art. 30.1). Y con todo ello actuará. Y responderá si decidió mal y produjo daños o se vulneraron derechos de los interesados. O no producirá daños, pero podrá haber gastado tanto dinero en seguridad que su cuenta de resultados se verá afectada[34].

En ese escenario, puede sorprender que no todos los profesionales del derecho entiendan la trascendencia de cifrar el fichero de clientes y la información confidencial proporcionada por ellos mismos o por sus contrapartes. Sin embargo, en nuestra experiencia, otras medidas que parecen tan lógicas, como implementar una política de mesas limpias, o almacenar los expedientes en soporte físico dentro de armarios ubicados en áreas de acceso protegido, con puertas cerradas con llave u otro dispositivo equivalente, tampoco se evidencian en todos los despachos.

Cuando tratamos con abogados, nos encontramos con que muchos de ellos equiparan seguridad de la información con confidencialidad, de suerte que si cifran la información (en algunos casos usando mecanismos poco fiables), tienen instalado un antivirus (algunos de ellos ni siquiera licenciado) y trabajan con el mismo personal en el que confían desde hace años, creen que están cumpliendo con sus deberes deontológicos y legales. No obstante, el uso de *software* antivirus no es suficiente para descubrir sofisticados ataques, que a veces no se detectan en un promedio de trescientos días[35].

En nuestra experiencia, en algunos despachos son comunes prácticas inseguras como no hacer copias periódicas de seguridad, o realizarlas en una USB o un disco duro externo, sin hacer pruebas de restauración (no solo se puede estropear, sino extraviar), no tener cifrada esa copia, no cerrar su despacho bajo llave, compartir información sensible usando cualquier servicio o aplicación que encuentren en internet, sin valorar sus riesgos, comunicarse con frecuencia con clientes y colaboradores por mensajería instantánea (WhatsApp o Telegram, entre otras) citando o adjuntando fotos o imágenes personales; imprimir documentos con información confidencial en cualquier copistería (sin cerciorarse del nivel de seguridad de sus redes, de la formación de su personal ni mucho menos firmar con ellos un contrato de encargado del tratamiento que

[34] *Ibid*.

[35] Karen Painter Randall y Steven A. Kroll, "Getting Serious about Law Firm Cybersecurity". *New Jersey Lawyer*, n.º 300 (junio del 2016): 56.

les exija borrar la información impresa de la memoria de sus equipos u otras medidas de seguridad pertinentes).

Estas son apenas algunas de las conductas inseguras más frecuentes entre los abogados que no han estudiado a profundidad la normativa vigente en materia de ciberseguridad y protección de datos personales o, al menos, no han recibido formación cualificada o investigado sobre ello. Cabe citar otras, como:

- No disponer de un inventario de activos de información coherente, sin el que resulta imposible determinar las medidas de seguridad necesarias.
- No contar con un análisis de riesgos metódico y ajustado a la realidad, que permita priorizar las medidas de seguridad necesarias y las modificaciones en los procedimientos de trabajo en el despacho.
- Contratar encargados del tratamiento o mantener los actuales sin solicitarles ninguna garantía de su parte en materia de seguridad de la información, ni verificar todas las medidas técnicas, organizativas y formativas que serían exigibles (lo cual es de esperar cuando ellos mismos no las han implementado, pero también sucede entre los despachos que sí lo han hecho y no se cercioran de que sus encargados también lo hagan).
- No formar correctamente a la plantilla del despacho en materia de ciberseguridad y protección de datos personales y secretos empresariales a nivel usuario. De hecho, si el empleado o becario firma dicho compromiso sin haber sido debidamente formado y, como consecuencia de ello, un incumplimiento ocasiona una pérdida o difusión ilegítima de la información, el convenio puede declararse directamente nulo por abuso de la posición de poder del empleador frente al empleado.
- No fijar reglas de utilización de dispositivos personales puestos al servicio de tareas profesionales con todo el personal de la oficina.
- No delimitar correctamente el ámbito en el que la información se puede difundir, bajo el "principio del mínimo conocimiento"[36].

[36] Consejo General de la Abogacía Española, Instituto de Ciberseguridad de España (Incibe) y Agencia Española de Protección de Datos (AEPD), *Cómo gestionar una fuga de información en un despacho de abogados* (Madrid: E-Book-Guías TIC, 2016), 12.

Según este, solo aquellos miembros del despacho que desempeñen una función que requiera acceso a la información, en parte o en su totalidad, deben tener la posibilidad de conocer su contenido, modificarlo o eliminarlo, tanto en papel como en formato electrónico. Esto solo se logra con una adecuada asignación de roles, personalizando los permisos por usuario, implantando técnicas de autenticación eficientes (por ejemplo, de doble *opt-in*), revisando periódicamente los permisos concedidos, revocándolos o eliminando usuarios cuando sea pertinente.

- Ausencia de tecnologías que contribuyan a proteger la información, evitando la entrada de correos contaminados o la salida de información sensible (del tipo *firewall*[37], *sandbox*[38] o DLP[39]), cuyos costes sean coherentes con las posibilidades presupuestarias del abogado o despacho.
- Del punto anterior se desprende otro muy importante: la falta absoluta de presupuestos de ciberseguridad en las cuentas anuales de los abogados o despachos.
- Ausencia de procesos definidos para la correcta gestión de una brecha de información, en caso de haberla.

Muchas de estas carencias se explican por el desconocimiento de los riesgos que enfrentan los activos de información y las consecuencias de su materialización. Algunos abogados creen que el riesgo es mayor cuanto más grande sea el negocio que gestionan y el volumen de personal de la empresa. Si bien es cierto que cuantas más personas involucradas, mayores probabilidades de brechas de información de origen humano, los ciberriesgos que enfrenta un despacho pequeño y uno grande son los mismos. Sin embargo, un despacho que lleve asuntos penales o especializados en violencia de género, por ejemplo, gestiona información

[37] *Firewall* o cortafuegos, cuya función es filtrar las comunicaciones, permitiendo las autorizadas y bloqueando las no autorizadas.

[38] *Sandbox*: mecanismo de seguridad que permite disponer de un entorno aislado del resto del sistema operativo aplicando el principio de que cuanto más alejados se frenen los riesgos, menos vulnerable será nuestra red.

[39] *Data loss prevention:* herramienta para controlar que los usuarios finales no envíen información sensible o crítica fuera de la red corporativa.

más crítica que uno que se especialice en reclamar comisiones injustificadas a los bancos.

Existen medidas tan novedosas como necesarias en la nueva normativa, tales como la de avisar a los afectados en setenta y dos horas acerca de la brecha de información, detallando el tipo de incidente ocurrido, los datos personales que se vieron comprometidos, las medidas técnicas, organizativas y formativas adoptadas para evitar que ocurriera y las que se adoptarán a partir del incidente para que no se repita[40]. Sin duda, para un abogado, llamar a un cliente a informarle que su expediente se le quedó en una cafetería y no pudo recuperarlo, que algunas de las pruebas que forman parte de la reserva del sumario fueron sustraídas por cibercriminales y él no las tenía cifradas, o incluso, que una de las pruebas que aportó fue borrada dolosa o accidentalmente y él no tenía copia de seguridad… mina por completo la confianza del cliente, que no solo querrá una subsanación sino un nuevo profesional de mayor diligencia que lleve sus asuntos.

Más grave todavía sería leer una comunicación pública, en la página web de la empresa (aunque muchos abogados no cuentan con una) o en un medio de comunicación masivo, en la que se diga que el prestigioso abogado Z. P. Q. o el prestigioso despacho X. W. Z. Abogados informa que ha sufrido un incidente de seguridad que puede poner en riesgo los derechos y libertades de sus clientes. Muy difícil resulta salir bien librados de tal experiencia y seguir adelante en su ejercicio profesional. Tal situación ocurriría en caso de que el esfuerzo para informar en setenta y dos horas a los afectados de manera fehaciente e individual fuese desproporcionado. ¿Pero, por qué la normativa somete al abogado a tal obligación que puede suponer el fin de su carrera? Para intentar proteger a las víctimas en el menor tiempo posible, dándoles la opción de tomar medidas reactivas como el cambio de contraseñas, la revocación de números de tarjeta e incluso cambiar de domicilio cuando pueda estar en juego su seguridad, por ejemplo, en casos de violencia de género, si el dato filtrado fuese su ubicación y la víctima estuviese huyendo del agresor.

[40] Agencia Española de Protección de Datos (AEPD) *Guía para la notificación de brechas de datos personales*, AEPD (2021), 22. https://www.aepd.es/es/documento/guia-brechas-seguridad.pdf.

El impacto de la brecha de seguridad puede ir desde una sanción administrativa o deontológica, hasta multas y consecuencias penales, pasando por el desprestigio del despacho y de los profesionales a quienes los clientes habían cedido su información amparados en el deber de secreto[41].

Si una fuga de información por sí sola puede ser nociva para el abogado, sus representados y sus empleados, una gestión deficiente de esta puede agravar mucho las consecuencias para cualquiera de ellos. Por ejemplo, si el personal no detecta señales de un funcionamiento deficiente de su equipo, que pueda ser causado por un ciberataque, y lo descubre de manera tardía, se pierde tiempo que puede ser vital para frenar la difusión de la información sustraída o minimizar el impacto sobre los afectados. Una rápida intervención permitiría bloquear usuarios hasta la asignación de nuevas claves, desindexar casi de inmediato determinados datos o imágenes de los buscadores o redes sociales (con la necesaria intervención de las autoridades), retirar información de medios de comunicación en línea o bloquear cuentas bancarias en caso de una suplantación de identidad con consecuencias económicas[42].

Al evaluar la cantidad y criticidad de información afectada será clave contar con el inventario actualizado de activos de información, puesto que de no tenerlo será difícil determinar quiénes son los afectados y en qué grado pueden poner en riesgo su libertad y dignidad, por ejemplo, impidiéndole acceder a un bien, ejercer un derecho, materializar un contrato o amenazando su seguridad e integridad o la de su familia.

Si el análisis no es certero, las medidas adoptadas para mitigar los riesgos pueden no ser efectivas, la propia valoración de la necesidad de reportar o no la brecha ante las autoridades y el propio Colegio de Abogados dependerá de la intuición, más que de la evidencia, y la capacidad de hacer un adecuado informe se verá afectada. Asimismo, será difícil determinar cuáles son las medidas necesarias para restaurar la resiliencia del sistema y evitar que las mismas vulnerabilidades se materialicen en el futuro.

[41] Consejo General de la Abogacía Española *et al*., *Cómo gestionar una fuga*, 18.

[42] Sobowale, "Six Major Law Firm".

Cibercompetencias y otras medidas exigibles a los profesionales de la legalidad

Cultura de la seguridad

Antes de definir las medidas que debe aplicar cualquier abogado en el ejercicio de sus funciones para proteger diligentemente los datos de carácter personal y la información proporcionada por sus clientes, resulta pertinente entender que muchas de las conductas inseguras en las que incurren los abogados obedecen a su grado de cultura en seguridad de la información[43].

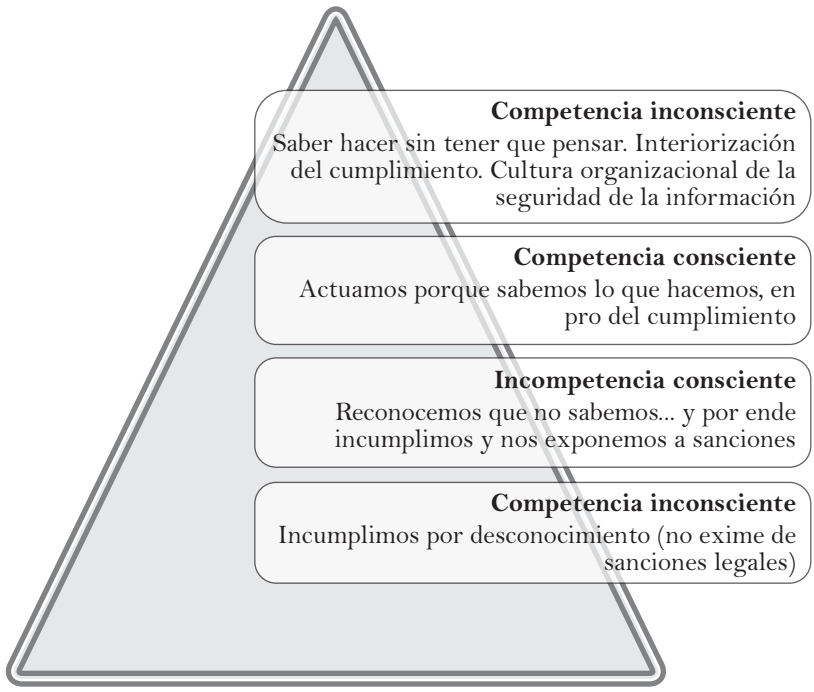
Si tenemos en cuenta que, más que ningún otro profesional, los abogados saben que el desconocimiento de la ley no exime de su cumplimiento, es difícil pensar que incumplan a sabiendas las medidas exigibles, por lo cual una incompetencia inconsciente no debería persistir a lo largo del tiempo. No obstante, las múltiples conductas inseguras citadas en la sección anterior obligan a una reflexión al respecto (véase la gráfica I.1).

Cuando el abogado o despacho abordan con personal interno o la asesoría pertinente un análisis de riesgos de su actividad, de sus procesos, del tipo de información que gestiona (coherentemente clasificada) y los tratamientos a los que la somete, de la legitimidad con la que recoge los datos de sus clientes, empleados u otros, para una finalidad específica, debe considerar tanto la probabilidad como la gravedad de que accidental o dolosamente sean conocidos por personal no autorizado; sean modificados, eliminados o sustraídos, o no estén disponibles cuando se requieren. A partir de este riguroso análisis, y de la clasificación de los riesgos identificados, deberá trazar un plan de acción que permita implantar medidas formativas, documentales, procedimentales y técnicas en función de los recursos humanos disponibles y de las soluciones vigentes en el mercado, priorizando aquellas que mitiguen o eliminen los riesgos más altos para la dignidad y las libertades de los interesados.

Sin duda, las acciones que por excelencia permiten aumentar el grado de cultura de la información de un abogado o despacho y todos los miembros de su equipo son las que se orientan a la concienciación y

[43] Jeimy Cano, "The Human Factor in Information Security: The Weakest Link or the Most Fatigued?", *ISACA Journal*, n.º 5, 2019.

Gráfica I.1. Grado de cultura en seguridad de la información y protección de datos personales



Fuente: Adaptado de Martin Broadwell. "Teaching For Learning (XVI.)", *The Gospel Guardian* 20, n.º 41 (1969): 1-3, http://www.wordsfitlyspoken.org/gospel_guardian/v20/v20n41p1-3a.html

formación, que serán más efectivas en la medida en que se acompañen de ciberejercicios (por ejemplo, simulación de *ransomware* y *phishing*), pues estos permitirán identificar a los usuarios más vulnerables, para incidir con ellos en los conocimientos que, a pesar de las jornadas o cursos en los que han participado, no han asimilado. Si se utilizan canales internos de comunicación para reforzar mensajes en torno a los nuevos procesos, el manejo de las nuevas tecnologías, la forma correcta de tratar la información, y las consecuencias de un incumplimiento doloso para el despacho y para el profesional mismo, se alcanzará en menor tiempo el estado de competencia consciente, y a medio o largo plazo con cursos de actualización, el de competencia inconsciente. Esta evolución no

solo es favorable para asegurar la continuidad de negocio, sino que además le permite ofrecer un servicio de alto valor agregado en el mercado.

La normativa es compleja y desafiante; por ende, su implementación se lleva a cabo paso a paso. Sin embargo, hay obligaciones relativas a la privacidad de la información que no provienen de la normativa reciente. El punto de partida es el "deber de guardar el secreto profesional por parte del abogado, incluso después de cesar la prestación de sus servicios"[44], que se ve reforzado con la obligación del abogado de "atender con celosa diligencia sus encargos profesionales, lo cual se extiende al control de los abogados suplentes y dependientes, así como a los miembros de la firma o asociados o abogados que represente al suscribir contrato de prestación de servicios y a aquellos que contrate para el cumplimiento del mismo"[45]; y aún más reforzado, en el sentido que nos atañe, con el "deber de abstenerse de incurrir en actuaciones temerarias"[46].

¿Acaso no es temerario que un abogado tenga una red insegura, débilmente configurada y compuesta por ordenadores en los que el sistema operativo y/o el *software* instalado no es original y, por tanto, no recibe las pertinentes y continuas actualizaciones de seguridad diseñadas por sus desarrolladores para mitigar los riesgos que se desprenden de vulnerabilidades conocidas?

¿No es temerario que personal sin ninguna formación en ciberseguridad ni cumplimiento normativo en materia de protección de datos personales tenga permisos de administrador y pueda descargar sin ninguna restricción aplicaciones, videos, música o documentos de cualquier fuente sin comprobar si es seguro o pueda venir acompañado de un troyano mediante el cual los ciberdelincuentes casual o causalmente (por encargo) puedan acceder a la información confidencial que el cliente le confió al abogado en cumplimiento de los deberes mencionados?

Considerando que la "aceptación de cualquier encargo profesional para el cual no se encuentre capacitado, o que no pueda atender diligentemente […]" está estipulado en el Código Disciplinario del Abogado

[44] Ley 1123/2007, 22 de enero del 2007, por la cual se establece el código disciplinario del abogado. *Diario Oficial* 46519.

[45] *Ibid*., art. 11.

[46] *Ibid*., art. 28.16.

en Colombia como una falta de lealtad con el cliente[47], ¿acaso no sería desleal que, por ejemplo, un abogado penalista del que depende una resolución justa para una víctima o un acusado que defiende su inocencia incurra en algunas de las conductas de riesgo recogidas en el apartado anterior, desconociendo la posibilidad de que dicha información sea alterada, sustraída o ilegítimamente publicada, dejando sin valor o posibilidad de probar los argumentos que planeaba esgrimir a favor de su cliente? Si tal cosa ocurriese, ¿no podría citarse el incumplimiento de sus obligaciones en materia de seguridad de la información y protección de datos personales como un criterio agravante[48] de la conducta negligente del abogado, en la medida en que afecta el derecho fundamental de proteger los datos de carácter personal de su representado, o de terceros vinculados en el proceso judicial o extrajudicial del que se ha hecho cargo?

¿Hasta qué punto puede considerarse esta conducta como negligente cuando el abogado desconoce los perjuicios que puede ocasionar su conducta?

Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas[49], el abogado, como responsable del tratamiento, debe asegurar a sus clientes la implantación de las medidas técnicas y organizativas que garanticen la seguridad de los datos personales y demás información confidencial cedidas por estos o relativas a ellos, de manera que evite la destrucción, pérdida o alteración accidental o ilícita de los datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Tales medidas deben ser, como mínimo, las especificadas a continuación:

a. Nombramiento de un responsable en materia de protección de datos, quien deberá asegurar el continuo cumplimiento de la normativa aplicable.
b. Establecimiento de funciones y responsabilidades del personal que trate datos de carácter personal.

[47] *Ibid.*, art. 34.i.

[48] *Ibid*., art. 45.c.2.

[49] RGPD, Reglamento (UE) 2016/679, arts. 24, 25 y 32.

c. Comunicación entre el personal de las funciones y responsabilidades definidas asociadas al cumplimiento de la normativa en materia de protección de datos.
d. Definición de roles y perfiles para los usuarios de las aplicaciones y sistemas donde se traten dichos datos, de acuerdo con las funciones y responsabilidades establecidas, de forma que se evite el acceso a datos o recursos distintos de los autorizados. Este sistema de control de acceso deberá aportar mecanismos adecuados de identificación y autenticación de los usuarios, por ejemplo, mediante el uso de contraseñas que han de ser renovadas de forma periódica, uso de datos biométricos, bloqueo automático de usuario ante intentos sucesivos fallidos de acceso, entre otros.
e. Medidas automatizadas que limiten el acceso a información para usuarios no autorizados o fuera del plazo de conservación determinado, por ejemplo mediante técnicas de borrado o de seudonimización de datos.
f. Procedimientos que limiten el acceso físico a las instalaciones donde se encuentren ubicados los sistemas o los soportes de información.
g. Registros de control y acceso sobre soportes que contengan datos de carácter personal, que además deberán contar con mecanismos de acceso limitado (por ejemplo, USB, discos externos o dosieres).
h. Procedimientos de recuperación de datos de carácter personal ante su posible destrucción, pérdida o alteración, bajo la supervisión y aprobación del responsable en materia de protección de datos.
i. Procedimientos de detección, evaluación y notificación, en caso de ser necesario, de incidentes de seguridad que puedan afectar los derechos y libertades de los interesados.

En todo caso, deberá implantar mecanismos específicos para:

a. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento[50].

[50] *Ibid*., art. 32.b.

b. Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico[51].
c. Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento[52].
d. Seudonimizar y cifrar los datos personales[53] cuando una violación de su confidencialidad, integridad o disponibilidad lleve asociado un riesgo que así lo sugiera.

Por otro lado, para que los medios de prueba previstos por el abogado surtan su efecto conforme a las normas del procedimiento penal, será menester demostrar su inviolabilidad, confidencialidad, integridad y disponibilidad. Todo ello requiere medidas de seguridad apropiadas, que todos los abogados partícipes en el proceso deberán aplicar en la parte que les corresponda.

¿Están los abogados "ciber-obligados"?

La propia American Bar Association (ABA) define los bufetes de abogados como objetivos "atractivos" y "blandos" para un ciberataque. En primer lugar, porque manejan una variedad de información de alto valor (fuertemente regulada), como propiedad intelectual, información privilegiada, información sobre transacciones y fusiones de empresas e información de salud protegida de clientes y otras partes involucradas en una demanda. En segundo lugar, pero no menos importante, porque frente a otras industrias no han dedicado una cantidad significativa de tiempo y dinero a asegurar que se implementen políticas y procedimientos suficientes para protegerse contra un ataque.

Para asumir una actitud proactiva de la ciberseguridad, es crucial que los bufetes entiendan los tipos de datos que están siendo atacados por *hackers*, así como las responsabilidades legales y éticas exigibles por sus clientes. Estos últimos cada día son más conscientes al respecto y

[51] *Ibid*., art. 32.c.

[52] *Ibid*., art. 32.d.

[53] *Ibid*., art. 32.a.

demandan medidas fehacientes para proteger su información confidencial, que garanticen que sus propios defensores legales no se conviertan en "puertas traseras" para los *hackers*[54].

Según esta misma entidad, las principales ciberamenazas que enfrentan los despachos de abogados son, en su orden, el *spearphishing* (correos maliciosos que, por medio de un adjunto o enlace, posibilitan a los delincuentes acceder a información de los clientes), el *ransomware* (virus que encripta la información de una organización a cambio de un rescate por su devolución, particularmente grave cuando no se cuenta con una copia de seguridad actualizada y fácilmente restaurable de los datos ilegibles) y el hacktivismo ideológico, que ataca sobre todo a firmas que defienden asuntos que implican un compromiso social, económico o medioambiental.

Si bien el cibercrimen crece a marchas forzosas, estos riesgos no son una novedad. En el caso de España, el propio Consejo General de la Abogacía Española definió en el 2012 la ciberseguridad como un "elemento indispensable en la estrategia del despacho"[55]. Mucho ha llovido desde entonces y el crecimiento del cibercrimen ha sido exponencial. Ante una complejidad de *trackers* sin precedentes en un mundo convulso en el que Estados Unidos y China luchan por el control de la banda ancha de quinta generación (5G), el nuevo orden jurídico-digital mundial es muy ambicioso y su dimensionamiento real, tras más de un año de entrada en vigor del RGPD, aún escapa a la comprensión de muchos profesionales, empresarios y particulares. Sin embargo, esta no puede ser la excusa del incumplimiento de los abogados, ante un escenario en el que "según reporte del Centro Cibernético Policial, el cibercrimen en Colombia tiene una tasa de crecimiento del 28,3 % año tras año y permanentemente aparecen nuevas amenazas para la seguridad cibernética que no solo atacan el bolsillo sino la invaluable privacidad de los ciudadanos"[56]. No obstante, todavía hay muchos despachos en los que la "seguridad de la información" no pasa de tener un papel accesorio y,

[54] Painter Randall y Kroll, "Getting Serious", 54-55.

[55] Consejo General de la Abogacía Española *et al*., *Cómo gestionar una fuga*, 4.

[56] Carlos Brand, "Empresarios invierten 190 000 millones al año para evitar el cibercrimen": Declaraciones del Sr. Jay García, arquitecto de la firma Controles Empresariales, *RCN Radio*, 1.º de julio del 2019, https://www.rcnradio.com/tecnologia/empresarios-invierten-190-mil-millones-al-ano-para-evitar-el-cibercrimen.

por ende, se encomienda a cualquier técnico informático, que en muchos casos no cuenta con los conocimientos necesarios para ser el garante de tan importante cometido.

Colombia adoptó en el 2008 la Ley 1266, en la que se dictan las disposiciones generales de *habeas data*, complementada en octubre del 2012 con la promulgación de la Ley 1581 de privacidad de datos, que eleva la protección de datos personales a un derecho fundamental, en el mismo sentido que Europa. Al igual que las leyes de Argentina y Uruguay, esta prohíbe la transferencia de datos a países que no cuentan con regímenes de protección de datos "adecuados" según lo determinado por el regulador colombiano[57], a menos que el sujeto de los datos otorgue su consentimiento previo, expreso e informado, o la compañía colombiana que vaya a transferir internacionalmente los datos obtenga una certificación de conformidad ante la SIC. Por su parte, la Ley 1273 del 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos, con penas de prisión de hasta ciento veinte meses y multas de hasta mil quinientos salarios mínimos legales mensuales vigentes. El avance legislativo en temas de *habeas data* se produjo con el Decreto 1377, que se promulgó en junio del 2013 y por el cual se establecieron obligaciones para responsables y encargados del tratamiento bajo el principio de responsabilidad demostrada (*accountability*).

Si bien en Colombia las cuantías de las sanciones son muy inferiores a las del RGPD y el alcance de la normativa en términos de políticas de privacidad o datos personales sensibles no alcanza los estándares de la UE, el país tiene hoy un marco regulatorio amplio y garantista en cuanto a protección de datos de carácter personal, ciberseguridad, privacidad e IT, reforzado con un exigente régimen sancionador para quienes vulneren dolosamente estos derechos y para quienes, aunque tienen el deber de tomar medidas para protegerlos, no lo hagan. La SIC constituye la máxima autoridad en materia de protección de datos, con la potestad de imponer multas de hasta dos mil salarios mínimos mensuales vigentes

[57] El RGPD también prohíbe las transferencias internacionales a países que no estén incluidos dentro de los declarados seguros por la comisión. "Destinatario declarado de nivel adecuado por la Comisión Europea", Agencia Española de Protección de Datos (AEPD), acceso el 9 de junio del 2021, https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales.

y suspender actividades en relación con el tratamiento de datos. Sin embargo, todavía queda un largo camino por recorrer si consideramos que entre los abogados aún no se asumen las cibercompetencias o la protección de datos personales como competencias transversales en todas las ramas del derecho, que de hecho han de ser mucho más exigentes entre los profesionales de las ramas penal y procesal, los que lleven casos de violencia de género, vulneración de derechos de menores de edad o discapacitados, o quienes gestionen información de testigos o peritos protegidos, víctimas de delito, información de carácter sanitario, religioso, ideológico, político, sindical o relativo a la orientación sexual de las personas, vedando el acceso a todas aquellas personas que no formen parte del procedimiento, salvo que acrediten un interés legítimo para ello[58].

Entre las medidas de las que no cabe duda que debe aplicar un abogado y que ya fue abordada al principio del capítulo está la de cifrar la información sensible proporcionada por los clientes. En España esa obligación la introdujo el artículo 104 del Reglamento 1720/2008, en el cual se especifica que únicamente son válidos los sistemas de cifrado que garantizan que la información no sea inteligible ni manipulada por terceros. En Colombia no existe esa especificación, pero uno de los principios sobre los que se cimienta el *habeas data* es el de seguridad, que establece que

> […] los datos personales e información usada, capturada, recolectada y sujeta a tratamiento, será objeto de protección en la medida en que los recursos técnicos y estándares mínimos así lo permitan, a través de la adopción de medidas tecnológicas de protección, protocolos, y todo tipo de medidas administrativas que sean necesarias para otorgar seguridad a los registros y repositorios electrónicos evitando su adulteración, modificación, pérdida, consulta, y en general en contra de cualquier uso o acceso no autorizado[59].

[58] Miguel Marcos Ayjón, "Las múltiples implicaciones de la protección de datos en la justicia penal", *La Ley Penal*, n.º 132 (junio del 2018): 6.

[59] Daniel A. López Carballo *et al*., "Protección de datos y *habeas data*: Una visión desde Iberoamérica", en *XVIII Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos*, coordinado por Daniel A. López Carballo (Madrid: Agencia Española de Protección de Datos, 2015), 40.

La obligación de cifrar por parte de cualquier abogado en el ejercicio de su profesión, respecto del fichero de clientes, está contemplada en los artículos 18 y 24 de la Constitución española y en el artículo 5 del Código Deontológico de España, pero es desconocida o mal interpretada por muchos profesionales de la rama legal.

A la AEPD se le consultó si los sistemas de cifrado de ciertas herramientas, como las de compresión de archivos, y los sistemas de claves de los PDF eran suficientes para cumplir la normativa. El gabinete jurídico de la agencia respondió con un no rotundo y añadió:

> Los productos que generan archivos PDF o el realizado por WinZip tienen vulnerabilidades conocidas y se dispone de herramientas de libre distribución que aprovechan dichas vulnerabilidades. Más concretamente, no solo se pueden obtener en internet fácilmente utilidades que rompen las protecciones de los archivos PDF o ZIP, sino que el propio algoritmo en el que descansa la cifra de documentos PDF, el algoritmo RC4, es manifiestamente vulnerable[60].

Al respecto, la AEPD concluye que

- Para un uso particular, los sistemas generales de cifrado (ZIP, PDF, etc.) podrían considerarse adecuados, según el caso.
- Para un uso profesional, los sistemas generales de cifrado son insuficientes para el intercambio de información con las garantías que se precisan legalmente. La respuesta para cumplir la normativa se encuentra en las herramientas profesionales pensadas, diseñadas y probadas para cumplir al detalle la normativa vigente en materia de cifrado[61].

A nuestro entender, este concepto emitido en el 2009 está más vigente que nunca pues todos los días los cibercriminales cuentan con más conocimientos y herramientas para vulnerar sistemas débiles de cifrado. Por esta razón, hay que recurrir a mecanismos de cifrado robusto para evitar

[60] Agencia Española de Protección de Datos, *Informe del Gabinete Jurídico* n.º 0494/2009.

[61] Abanlex, *Primer informe*, 5.

que terceros no autorizados accedan a la información y a alternativas como el *hashing* cuando el propósito sea validar que un contenido es fidedigno y no ha sido modificado sin necesidad de recuperar el contenido.

La AEPD cita alternativas al cifrado de datos, como son la esteganografía para la ocultación de mensajes a nivel de aplicación o la transmisión mediante espectro ensanchado (*spread-spectrum*) para el caso inalámbrico a nivel físico[62]; todas ellas con una implementación y una gestión mucho más compleja y problemática que la que ofrecen los actuales sistemas de cifrado. Pero no solo es necesario cifrar, sino hacerlo de tal manera que la información no sea inteligible ni manipulada por terceros. Esto implica dos cosas: por un lado, que el sistema de cifrado por emplear no esté comprometido, es decir, que en el momento de implementarlo no se conozca forma de romperlo, por otro lado, que se cuente con un sistema de gestión de claves[63].

Haciendo referencia a la nueva normativa, el considerando 83 del RGPD establece que

> A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el Responsable o el Encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado […] teniendo en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales[64].

No cabe duda, entonces, de que los abogados están obligados a cifrar para cumplir sus obligaciones legales y deontológicas, y el mecanismo seleccionado debe ser robusto, por engorroso o costoso que parezca. No hay datos específicos del cumplimiento de estas obligaciones en el caso

[62] Con la *esteganografía* el emisor oculta mensajes a nivel de aplicación para enviarlos en forma de imágenes por medios electrónicos, incluido el satelital. Por su parte, el sistema de transmisión mediante espectro ensanchado permite el envío de mensajes ocultos para el caso inalámbrico a nivel físico.

[63] Abanlex, *Primer informe*, 4.

[64] RGPD, Reglamento (UE) 2016/679, Considerando 83.

colombiano, por lo que debemos remitirnos a reportes a escala mundial. Según el *ABA Tech Report 2019* del American Bar Association Legal Technology Resource Center, los abogados están fracasando en materia de ciberseguridad. Sorprendentemente, los resultados reflejan poco o ningún movimiento positivo en el último año, o incluso en los últimos, hasta el punto de convertirse en un motivo de preocupación en la profesión. Los datos resultan reveladores: la medida de seguridad más popular utilizada por el 35 % de los abogados encuestados es el cifrado SSL. Solo el 27 % de ellos hace copias de seguridad de datos locales. Desde el 2018, en lugar de crecer el interés por las políticas de seguridad de sus proveedores, el porcentaje que las lee cayó del 38 % al 28 %, y lo más incoherente de todo es que a pesar de que el 94 % dijo que la reputación del proveedor importaba a la hora de decidir con quién contratar, apenas un 23 % investigó el historial de este. Respecto a los servicios en la nube, su contratación en los despachos legales aumentó de un 55 % a un 58 % en el último año, pero solo la cuarta parte declaró haber revisado opiniones éticas relacionadas con este tipo de tecnología. Por último, cabe destacar que algo más de un cuarto de los encuestados (26 %) informó que su empresa había tenido una brecha de seguridad[65].

Esta situación refleja el desconocimiento por parte de los abogados del principio de responsabilidad proactiva que los obliga a seleccionar únicamente encargados del tratamiento que cumplan las medidas de seguridad exigidas por ellos como responsables y a implementar la privacidad por defecto y desde el diseño en todos sus procesos y tratamientos, máxime cuando se refieran a información sensible como la que ellos gestionan.

Otra novedad del sistema normativo digital introducido por el RGPD es la referencia expresa a la posibilidad de que el responsable del tratamiento audite al encargado[66], lo que implica un riesgo para los abogados que no hayan introducido las medidas técnicas, organizativas, formativas y documentales pertinentes y no las actualicen conforme se modifiquen

[65] Jason Tashea, "Lawyers Are Failing at Cybersecurity, Says *ABA Tech Report 2019*", *ABA Journal* (24 de octubre del 2019), http://www.abajournal.com/news/article/lawyers-are-failing-at-cybersecurity-says-aba-techreport-2019.

[66] RGPD, Reglamento (UE) 2016/679, art. 28.3.h.

los riesgos[67], puesto que, "tanto el Responsable como el Encargado deben establecer un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas adoptadas para garantizar la seguridad del tratamiento"[68]. Una forma de evitar la auditoría o salir bien librado de ella puede ser implementar sistemas de gestión de seguridad de la información, como propone el propio RGPD cuando establece que la adhesión a un código de conducta aprobado por las autoridades de protección de datos o a un mecanismo de certificación como la ISO 27001 podrá servir de elemento para demostrar el cumplimiento de los requisitos consagrados en la norma[69]. No obstante, la mayoría de los despachos de abogados no cuenta con los recursos humanos y financieros para afrontar un estándar tan ambicioso como este. Aun así, sería recomendable crear algún estándar más básico para los abogados, que se adapte más a sus posibilidades, considerando el alto nivel de riesgos que enfrentan. "Al igual que el riesgo financiero y de reputación, el riesgo de ciberseguridad afecta al resultado final del despacho. Puede aumentar los costos e impactar los ingresos. Puede dañar la capacidad de la organización para innovar y para ganar y mantener clientes"[70].

Los abogados no son ajenos a la obligación de incorporar en sus servicios la privacidad desde el diseño y por defecto para dar garantías a los usuarios en cuanto al ejercicio de sus derechos y la seguridad de sus

[67] Ese riesgo se evidencia en que más del 50 % de las firmas de abogados encuestadas por LogicForce han sido auditadas al menos una vez en el último año por un cliente actual o potencial y en que, según ese mismo estudio, las exigencias de ciberseguridad de los clientes a sus firmas legales están creciendo, tanto en materia de medidas técnicas como de la formación del personal que trata su información. En el 2019 el número de bufetes que formalizaron sus políticas de privacidad aumentó del 55 % al 70 %, pero aportar garantías en cuanto a la seguridad de la información aún no se considera una prioridad estratégica y hay muchas carencias en la monitorización del riesgo. Véase "Law Firm Cybersecurity Score Card 2019", LogicForce, 2019, https://www.logicforce.com/2019/10/07/cyber-security-scorecard-q4-2019/.

[68] RGPD, Reglamento (UE) 2016/679, art. 31.1.

[69] *Ibid.*, art. 32.3.

[70] Sarah Jane Hughes, "Did the National Security Agency Destroy the Prospects for Confidentiality and Privilege When Lawyers Store Clients' Files in the Cloud and What, if Anything, Can Lawyers and Law Firms Realistically Do in Response?". *Articles by Maurer Faculty*, n.º 1342 (2014): 435.

datos personales[71]. La confidencialidad de determinadas informaciones, como la remuneración y las bonificaciones percibidas por los empleados, debidamente asociados a sus datos de identificación en investigaciones sobre discriminación salarial por razón de sexo u origen racial, obliga al abogado a dar acceso al perito a esta información directamente en la empresa investigada para que la analice y saque sus conclusiones, evitando su transmisión por fuentes externas para evitar su manipulación y/o la difusión a terceros. Así, si bien el juez o el árbitro no pueden acceder a la tabla salarial, el trabajo pericial garantiza la integridad de las fuentes y la fiabilidad de sus resultados. Este es solo un ejemplo de privacidad desde el diseño en el proceso pericial de acuerdo con el RGPD.

En cuanto a investigaciones sobre conductas dolosas de un empleado en particular, como la cesión de secretos empresariales a la competencia, hay que partir de los criterios de utilización de dispositivos digitales definidos en la política de la empresa, puesto que el ordenador asignado al trabajador investigado podría contener información personal de carácter sensible, como fotos familiares, resultados de pruebas médicas o temas financieros. A este respecto, el artículo 87 de la LOPDGDD sobre el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral establece que "los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador"[72]. No obstante, "el empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos"[73]. Esta nueva normativa de garantía de derechos digitales recientemente implantada en España[74] obliga a los empleadores a "establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos

[71] Instituto de Ciberseguridad de España (Incibe). *Ganar en competitividad cumpliendo el RGPD: Una guía de aproximación para el empresario* (Instituto de Ciberseguridad de España [Incibe] 2018), 29.

[72] LOPDGDD, art. 87.1.

[73] *Ibid.*, art. 87.2.

[74] *Ibid.*, título X, arts. 79-97.

reconocidos constitucional y legalmente, en cuya elaboración deberán participar los representantes de los trabajadores"[75], y de los cuales deberán ser fehacientemente informados los empleados.

Ahora bien,

> […] el acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados[76].

Medidas contractuales, que a su vez especifican las medidas técnicas exigibles

En esta área resulta exigible la firma de un contrato entre el abogado como responsable del tratamiento y cada uno de sus encargados del tratamiento y, a la vez, el abogado o despacho, en su calidad de encargado del tratamiento, deberá firmar contratos con sus clientes. En ambos casos, el objeto es definir las condiciones en virtud de las cuales el encargado del tratamiento llevará a cabo el tratamiento de datos personales necesario para la correcta prestación de los servicios proporcionados al responsable del tratamiento, que incluya[77]:

- La finalidad del encargo de tratamiento. En el caso de proveedores serán, por ejemplo, servicios informáticos, gestión fiscal, laboral, financiera, servicios de *marketing*, aplicaciones contables, CRM y ERP. En el caso de clientes,

[75] *Ibid.*, art. 87.3.

[76] *Ibid.*

[77] Agencia Española de Protección de Datos (AEPD), Autoridad Catalana de Protección de Datos (APDCAT) y Agencia Vasca de Protección de Datos, *Directrices para la elaboración de contratos entre responsables y encargados del tratamiento* (Madrid: 2017), 6-18.

> […] la defensa letrada del cliente en los asuntos judiciales y extrajudiciales que le encomienden sus representados, así como el desarrollo de dichas actividades; documentación de expedientes; facturación, cobro, gestión económica y contabilización de los servicios contratados; conservación de dichos expedientes durante su tramitación y a efectos de responsabilidad profesional; comunicación con el cliente, contrapartes y asesores[78].

- Concreción de los tratamientos por realizar, y de la tipología de datos de carácter personal que administrará en nombre del responsable del tratamiento, y categorías de interesados cuyos datos serán tratados por el encargado.
- Destino y plazo de conservación de los datos. En el caso de los abogados, los destinatarios más habituales serán los juzgados y tribunales, notarías, registros públicos, el letrado de la contraparte, entidades financieras, administraciones públicas y cuerpos y fuerzas de seguridad. En cuanto a los plazos de conservación de los datos contenidos en los expedientes derivados de los servicios profesionales prestados, los abogados deberán ceñirse a los plazos legales de prescripción (de acuerdo con el Código Civil o la ley de enjuiciamiento criminal); a efectos de facturación, a los plazos dispuestos en el Código de Comercio; a efectos de pagos de impuestos, a los plazos definidos en la ley general tributaria; y a efectos de cobro, hasta hacerlo efectivo[79].
- Base legítima del tratamiento encargado. En el caso de los abogados con sus clientes, por lo general aplica la ejecución de un contrato, del que el interesado es parte.
- Obligaciones del encargado del tratamiento, entre las cuales se recogen:
  - Llevar, por escrito, un registro detallado de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable del tratamiento, de conformidad con las exigencias

[78] Alfonso Pacheco Cifuentes, "El abogado ante el deber de información a sus clientes y el nuevo Reglamento General de Protección de Datos", *La Ley*, n.º 8804, 15 de julio del 2016, 5.

[79] *Ibid*., 5-6.

normativas, que incluya, entre otros aspectos, la descripción de las medidas técnicas y organizativas de seguridad relativas a

a. La seudonimización y el cifrado de datos personales.
b. La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
c. La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
d. El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

- No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa y por escrito del responsable del tratamiento, en los supuestos legalmente admisibles.
- No subcontratar ninguna de las prestaciones que formen parte del objeto del contrato que comporten el tratamiento de datos personales. (Establecer procedimiento y plazo para autorizar subcontrataciones que resulten necesarias y responsabilidad, en caso de permitirse una subcontratación del cumplimiento del subencargado de las mismas obligaciones que el encargado).
- Apoyar al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, así como en las consultas previas a la autoridad de control.
- Demostrar el cumplimiento de sus obligaciones legales y contractuales.
- Permitir y contribuir a la realización de auditorías e inspecciones por parte del responsable o un tercero autorizado por él.
- Notificar en tiempo y forma las violaciones de la seguridad de los datos.
- Asistir y dar apoyo al responsable del tratamiento en la respuesta al ejercicio de derechos por parte de los interesados.
- Deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de finalizar la relación contractual.

    - Formar en materia de protección de datos personales a quienes estén autorizados para su tratamiento.
    - Convenios de confidencialidad y cumplimiento normativo de las personas autorizadas para tratar datos personales, propios del encargo de tratamiento.
- Obligaciones del responsable del tratamiento.
- Consecuencias del incumplimiento del contrato en cualquiera de sus puntos.
- Legislación y fuero aplicable.

Medidas organizativas

"Para crear valor, los datos necesitan moverse, y para moverse se requiere la confianza de todos los agentes que participan en la cadena de valor"[80]. Los procesos del despacho deberán rediseñarse bajo el principio de privacidad y protección de datos desde el diseño y por defecto. El principio de *privacy by design* se basa a su vez en siete principios fundamentales[81] e implica que solo sean tratados los datos personales estrictamente necesarios para el cumplimiento de la finalidad específica para la que fueron recogidos, cumpliendo las disposiciones de la normativa vigente[82].

Los abogados deberán implementar medidas como la correcta clasificación de activos de información en función de su criticidad, la política

[80] Elena Gil, "*Big data*, privacidad y protección de datos". *XIX Edición del Premio Protección de Datos Personales de Investigación* (Madrid: Agencia Española de Protección de Datos, 2015), 138.

[81] Estos principios son: (1) Proactividad, no reactividad ni correctividad; (2) privacidad como la configuración predeterminada; (3) privacidad incrustada en el diseño; (4) funcionalidad total —todos ganan—; (5) seguridad de extremo a extremo —protección del ciclo de vida completo—; (6) visibilidad y transparencia —la información sobre políticas y prácticas referidas a la gestión de la información personal debe ser fácilmente accesible para los interesados—; y (7) respeto por la privacidad de los usuarios —mantener el enfoque centrado en los usuarios—. Miguel Recio Gayo, "Una aproximación a la aplicación del Reglamento (UE) 2016/679 sobre protección de datos (RGPD) al sector de la abogacía y despachos profesionales", en *Trabajo y derecho: Sección Práctica Jurídica y Despachos Profesionales* (Wolters Kluwer, 2018), 9.

[82] Véase AEPD, *Guía de privacidad desde el diseño* (2019), https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf.

de mesas limpias, la eliminación de datos personales atendiendo los plazos legales (o los pactados con los interesados), la *seudoanonimización* temprana de los datos personales y cualquier otra necesaria[83] para proteger los derechos y libertades de los titulares de los datos, de manera que estén en condiciones de demostrar su responsabilidad proactiva en la protección de datos de carácter personal.

La garantía de derechos digitales

Cuando hablamos de derechos digitales podemos pensar en respetar los horarios de trabajo de los trabajadores, procurando su conciliación familiar, o en la necesaria educación que deben recibir nuestros menores para no ver vulnerada su dignidad en las redes sociales. Ciertamente tiene que ver con esto, pero va mucho más allá y a los profesionales del derecho les afecta de maneras diversas.

Por un lado, como empleadores que deben asegurar a sus trabajadores el derecho a la desconexión digital, a ser informados de las finalidades de la videovigilancia (cuando esta pueda ser usada para el control laboral), de la geolocalización (cuando recurra a ella) y del *derecho a la intimidad y el uso de dispositivos digitales en el ámbito laboral.* Un bufete no deja de ser una empresa u organización obligada a cumplir con todo el entramado legal en torno a protección de datos personales, privacidad, ciberseguridad y delitos informáticos, por lo que en el propio despacho del juez o profesional del derecho sería deseable, en razón de la sensibilidad de información que se maneja, limitar el uso de los ordenadores, teléfonos o *tablets* a fines profesionales, pues a pesar de la costumbre social de consultar redes sociales en horario laboral, el hacerlo desde los dispositivos de la empresa entraña riesgos adicionales.

[83] La AEPD ha publicado una "lista no exhaustiva y con carácter orientativo, de aquellas opciones en las que un tratamiento podría ser configurable para implementar las medidas con relación a la cantidad de datos personales utilizados, la extensión del tratamiento, el periodo de conservación, la accesibilidad de los datos y cualquier otra circunstancia en el proceso del tratamiento susceptible de incidir en la privacidad de los usuarios". Véase Agencia Española de Protección de Datos (AEPD), *Guía de protección de datos por defecto* (2020), https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf.

Por otro lado, como parte o contraparte en un proceso judicial o extrajudicial de carácter laboral, basado en la vulneración de estos derechos, el abogado necesita comprender claramente la normativa que garantiza los derechos digitales para poder aplicarla en justicia.

Y finalmente, desde un punto de vista procesal, dado que para declarar la validez de las pruebas periciales hay que partir de la necesidad de hacer que sean suficientemente reproducibles para que un tribunal las considere válidas. Esto está directamente relacionado con la integridad, exactitud, licitud del tratamiento y transparencia de la información que constituye la prueba y que a menudo —por no decir que todas las veces— va asociada a datos personales de los presuntos infractores. Todo ello está íntimamente ligado con el tratamiento otorgado a dicha información para llegar a una conclusión por parte del perito.

En algunas ocasiones, esta "reproducibilidad" choca con la comprometida confidencialidad de las fuentes de las que se obtiene la prueba, bien porque pueda vulnerar el derecho fundamental a la protección de datos personales o porque la propia información "sensible" de la que se trate sea considerada un secreto empresarial del que dependa la ventaja competitiva de la empresa en el mercado[84].

En referencia a las pruebas obtenidas mediante videovigilancia, el artículo 89 de la LOPDGDD[85], sobre el derecho a la intimidad frente al uso de dispositivos de videovigilancia y grabación de sonidos en el lugar de trabajo, establece que

> […] los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa,

[84] Juan J. Valderas, "Cómo proteger la confidencialidad de información comercial o personal 'delicada' necesaria para la prueba pericial en un litigio", *La Ley*, n.º 8925 (2017).

[85] LOPDGDD, art. 89.

> clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida[86].

Entonces, si la cámara captó la comisión flagrante de un ilícito se entenderá cumplido el deber de informar a los empleados de esta medida cuando se incluya "un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento"[87].

En referencia a otras pruebas obtenidas de dispositivos digitales, hay que partir del análisis de la propiedad de estos. Por primera vez, los criterios de utilización de dispositivos de propiedad de la empresa deberán tener en cuenta el uso o la costumbre, es decir, los hábitos que pueden considerarse socialmente asumidos. Desde nuestro punto de vista, el juez deberá sopesar si el trabajador estaba autorizado para guardar su información personal o consultar su correo personal o sus redes sociales en los dispositivos de la empresa, o si existía una política BYOD[88] (*bring your own device*) que le indicara las precauciones de seguridad que debía tener su dispositivo personal para poder darle un uso compartido con fines profesionales. El juez también deberá indagar si estaba autorizado para utilizar determinados programas que estaban instalados en su ordenador, si tenía privilegios de administrador, si existía una instrucción respecto a la descarga o el uso de programas o una lista blanca de aplicaciones autorizadas… y de qué forma fehaciente y cuándo ha sido comunicado al trabajador en cuestión la política que contiene todas estas instrucciones. Si la investigación fuese relativa, por ejemplo, a la filtración de información privilegiada a la competencia, todo lo anterior deberá tenerse en cuenta para determinar si ocurrió de forma dolosa y consciente, o si inconscientemente, al incumplir la política de seguridad de la empresa, ha facilitado que ciberdelincuentes al servicio de la competencia o de grupos criminales accedan a la información.

[86] *Ibid.*

[87] *Ibid.*

[88] Instituto de Ciberseguridad de España (Incibe), *Dispositivos móviles personales para uso profesional (BYOD): Una guía de aproximación para el empresario* (2017), https://www.incibe.es/protege-tu-empresa/guias/dispositivos-moviles-personales-uso-profesional-byod-guia-aproximacion-el.

En cumplimiento de la garantía de los derechos digitales en el ámbito laboral, en el caso de aportar como pruebas correos electrónicos emitidos desde la dirección corporativa del trabajador, el juez solo podrá legitimarlos cuando el interesado haya sido previamente informado, el empresario pueda justificar la medida de monitorizar su correo y no exista otro método menos intrusivo para acceder a la información aportada.

Otro aspecto fundamental que el juez deberá tener en cuenta es el grado de formación recibido por el trabajador en materia de seguridad de la información. A menudo las empresas redactan documentos de confidencialidad que incluyen medidas de ciberseguridad con vocabulario técnico y los pasan a los empleados para su firma, creyendo que con ello cumplen las exigencias legales. Lo hemos evidenciado en numerosas ocasiones. No obstante, las autoridades de protección de datos pueden invalidar el contenido de estos contratos si consideran que el empleador está abusando de su posición dominante frente al trabajador, comprometiéndolo a cumplir unas exigencias que no entiende. Si el juez que tuviese asignado el caso, a pesar de su amplia y afamada trayectoria en la rama laboral, no entendiese las implicaciones de la normativa en protección de datos personales en cuanto a ciberseguridad (por ejemplo, si no comprendiese el porqué la descarga de un *software* no permitido podría conllevar un riesgo para la información sensible de la empresa; si no supiese interpretar una política BYOD o no supiese por qué la descarga de aplicaciones sin licencia en el móvil personal en el que consulta el correo de la empresa y guarda información de clientes —más allá de la propia vulneración de la propiedad intelectual de sus autores— entraña un riesgo en sí mismo por el hecho de que, cuando no se paga la respectiva licencia, las aplicaciones no pueden actualizarse oportunamente), no podría ejercer sus funciones con la debida imparcialidad. Son incontables los casos que pueden darse, en las distintas facetas de ejercicio de un profesional del derecho, que demuestran la necesidad de desarrollar unas competencias básicas en materia de ciberseguridad y protección de la privacidad. Necesitan una formación orientada a su manejo de información sensible que, por supuesto, debe ser continua, por cuanto los ciberriesgos evolucionan permanentemente conforme se hace más rentable el negocio del cibercrimen.

Siguiendo con la investigación de nuestro ejemplo, una vez clarificada la política de la empresa respecto a la utilización para fines privados de los dispositivos empresariales, el perito deberá proceder a buscar

evidencias en los activos de información usados por el empleado investigado del posible traspaso de información confidencial a la competencia, mediante una copia forense, cuya integridad se asegure con una adecuada cadena de custodia. De no existir una política clara de uso de equipos de la empresa por parte de los empleados, el perito deberá proceder a analizar la información mediante búsquedas ciegas de términos directamente relacionados con la brecha de información, para evitar acceder a información personal del trabajador no relevante para el caso[89]. Queda claro que el deber de secreto que rige la ética del abogado, marcando deberes legales y deontológicos, sumado a la propia definición de la profesión, obliga a los profesionales del derecho a implementar estrictas medidas de seguridad de la información proporcionada por los clientes y cualquier dato personal proveniente de terceros, especialmente cuando su difusión, alteración, conocimiento por terceros no autorizados o eliminación pueda suponer una amenaza para los derechos y libertades de un ser humano.

Asimismo, la garantía de los derechos digitales, aún no reglamentada en Colombia, recientemente fue regulada en España para proteger a empleados, menores, colectivos en riesgo de exclusión, a los ciudadanos como usuarios de internet y determinar en general los derechos de la era digital y las comunicaciones. Esto ha impactado directamente las relaciones laborales, los contenidos educativos impartidos en colegios y universidades, la interacción en redes sociales y las comunicaciones por medios digitales. Por lo tanto, la jurisprudencia deberá tener en cuenta —más allá de la propia regulación— las políticas implementadas en la materia para legitimar, en cada empresa, las pruebas aportadas de cara a determinar el grado de culpabilidad de un trabajador, responsable o encargado del tratamiento en una brecha de información y en sus posibles consecuencias. Es de esperar que la legislación colombiana siga estos pasos, por cuanto la interacción con el mundo digital y los riesgos que de ella se derivan están ampliamente extendidos en todos los colectivos sociales del país. También es previsible que la LOPDGDD requiera continuas actualizaciones por el surgimiento y la consolidación de nuevas

[89] Antonio Evaristo Gudín Rodríguez-Magariños, "La protección de datos en el tratamiento procesal de los dispositivos de almacenamiento masivo de información", *La Ley Penal*, n.º 125 (abril del 2017), 7 y 9.

tecnologías no contempladas en la norma, tales como los *smart contracts* y el propio 5G, que, más allá de poner en riesgo los datos de carácter personal, pueden representar peligros inminentes para la libertad y dignidad de cada ser humano y la sociedad en su conjunto[90].

El papel de la academia

Colombia ostenta el honor de incluir seis facultades entre las veinte mejores escuelas de Derecho en Latinoamérica según el escalafón internacional de la prestigiosa consultora educativa Quacquarelli Symonds (QS) en el 2021 (véase la tabla I.1).

Al analizar los programas académicos de cada una de ellas, sorprende que a pesar de ser una norma exigible a abogados de todas las ramas (teoría jurídica, derecho público administrativo, derecho público constitucional, derecho laboral, derecho penal, derecho procesal y derecho internacional), sin perjuicio de que puedan tocarse tangencialmente temas sobre ciberseguridad en materias como derecho procesal, derechos del consumidor, o en las relativas a las obligaciones deontológicas del abogado, no se encuentran asignaturas relativas a la seguridad de la información en ninguno de los pénsums académicos de pregrado analizados.

En la Universidad de los Andes no se incluye ninguna materia específica de ciberseguridad o protección de datos personales en sus estudios de pregrado, cinco especializaciones y cuatro maestrías[91,92], pero dentro de su oferta de Educación Continua, en el apartado "Actualización profesional en Derecho" hay cinco cursos muy relevantes: Protección de Datos y *Accountability*[93] (de 24 h), Ciberseguridad para Ejecutivos[94]

[90] Mayor Gómez, "Principales novedades", 55.

[91] *Catálogo general Facultad de Derecho*, Universidad de los Andes, https://catalogo.uniandes.edu.co/es-ES/2014/Catalog/School-of-Law/Undergraduate/Law-Degree.

[92] Especializaciones Facultad de Derecho, Universidad de los Andes, https://derecho.uniandes.edu.co/es/especializaciones.

[93] Programa de Educación Continua Universidad de los Andes en Protección de Datos y *Accountability*, https://educacioncontinua.uniandes.edu.co/es/programas/proteccion-de-datos-y-accountability.

[94] Programa de Educación Continua Universidad de los Andes en Ciberseguridad para Ejecutivos, https://educacioncontinua.uniandes.edu.co/es/programas/ciberseguridad-para-ejecutivos-retos-y-riesgos-en-el-contexto-digital.

Tabla I.1. Escalafón QS 2021 de universidades para estudiar Derecho en Colombia

Universidad	Escalafón QS Colombia	QS Latam	QS Law mundial	Puntuación QS
Universidad de los Andes Bogotá, Colombia-5 QS Stars	1	4	45	74,4
Universidad Externado de Colombia Colombia-4 QS Stars	2	7	92	68,9
Pontificia Universidad Javeriana Bogotá, Colombia	3	9	101-150	N. D.
Universidad del Rosario Bogotá, Colombia-4 QS Stars	4	10	101-150	N. D.
Universidad Nacional de Colombia Bogotá, Colombia-5 QS Stars	5	11	101-150	N. D.
Universidad de la Sabana Bogotá, Colombia	6	20	251-300	N. D.

Fuente: Tomado de "Ranking QS 2021 de universidades para estudiar Derecho en América Latina", Quacquarelli Symonds, https://www.topuniversities.com/university-rankings/university-subject-rankings/2021/law-legal-studies

(de 30 h) y Riesgos de la Empresa y el Empresario Frente al Derecho Penal[95] (de 20 h) y se incluye un apartado de criminalidad informática dentro de "Temas adyacentes". En la Escuela de Verano ofrece un curso sobre el papel del derecho en la gobernanza de los datos, la protección de la privacidad, la garantía de la transparencia algorítmica y la IA justa, la garantía de la competencia y el fomento de la innovación en la

[95] Programa de Educación Continua Universidad de los Andes en Riesgos de la Empresa Frente al Derecho Penal, https://educacioncontinua.uniandes.edu.co/es/programas/riesgos-de-la-empresa-y-el-empresario-frente-al-derecho-penal.

economía de la información digital, denominado *Data Governance in the Digital Economy*[96].

La Universidad de los Andes también ha ofrecido Los Riesgos del Uso de las Tecnologías para Empresas e Individuos[97] (de 32 h); *Legal Tech*[98] (de 44 h); Cibercrimen Digital[99] (de 30 h) y Seminario de Excelencia Tecnologías Disruptivas para Ejecutivos: Ciberseguridad, Criptografía, Firmas Digitales, *Blockchain* y *Bitcóin* (de 8 h).

En la Universidad Javeriana tampoco se incluye, ni entre las materias troncales ni entre las complementarias del pregrado, ninguna específica de seguridad de la información o protección de datos personales, temas que tampoco se abordan en sus doce especialidades y cinco maestrías[100]. Sin embargo, ofrece el Diplomado en Derecho Digital, del Entretenimiento y de la Innovación que incluye un módulo (entre quince) de Protección de Datos Personales (*Habeas data*, Contexto mundial-Sistemas de protección de datos personales, Régimen colombiano de protección de datos personales, Transferencia de datos personales, Procedimiento ante la SIC), otro de Delitos informáticos (Monitoreo en la red, Trazabilidad en la red, Ciberseguridad y Ciberdefensa) y el de Derecho Procesal y Probatorio en un Entorno Digital: Una Aproximación al Código General del Proceso y el Aporte de Evidencia Digitales (Derecho procesal y TIC; Código general del proceso; Evidencia forense digital; Pruebas en un entorno digital y Régimen probatorio).

[96] Programa de Educación Continua Universidad de los Andes en *Data Governance in a Digital Information Economy*, https://educacioncontinua.uniandes.edu.co/es/programas/data-governance-digital-information-economy.

[97] Programa de Educación Continua Universidad de los Andes en Riesgos en el Uso de las Tecnologías para Empresas e Individuos, https://educacioncontinua.uniandes.edu.co/es/programas/curso-los-riesgos-en-el-uso-de-las-tecnologias-para-empresas-e-individuos.

[98] Programa de Educación Continua Universidad de los Andes en Legal Tech, https://educacioncontinua.uniandes.edu.co/es/programas/curso-legaltech.

[99] Programa de Educación Continua Universidad de los Andes en Cibercrimen Digital, https://educacioncontinua.uniandes.edu.co/es/programas/curso-cibercrimen-digital-retos-y-perspectivas-juridicas-y-tecnologicas-emergentes.

[100] Plan de Estudios, Facultad de Derecho, Pontificia Universidad Javeriana, https://www.javeriana.edu.co/documents/153575/0/09-MAY-2018+Plan+de+estudios+Derecho/a8446a28-32da-4a58-9fec-f4bb949e0bf3.

De forma puntual, ofrece un curso gratuito certificable de Protección de Datos Personales en la Era Digital[101] dirigido a cualquier profesional. La Javeriana cuenta también con un Diplomado en Seguridad Informática, ISO 27000 Infraestructura, tecnología, productividad y ambiente[102], cuyo objetivo es conocer los principios de seguridad informática, técnicas de *hacking* y capacitarse en la norma ISO 27000, *pero no está dirigido a profesionales del derecho* sino a ingenieros de sistemas, auditores y otros profesionales interesados en temas de seguridad y auditoría de tecnologías de la información.

En el pregrado de Derecho de la Universidad Externado de Colombia no se comprenden estas materias dentro de la formación troncal, pero existe la opción de cursar una intensificación de tres horas semanales, de Derecho informático, cuyo objetivo es que

> [...] el estudiante comprenda y desarrolle una visión crítica y propositiva sobre la informática jurídica, los delitos informáticos, la protección de datos personales, las redes sociales, la seguridad de los sistemas de información, la responsabilidad derivada de las nuevas tecnologías, la regulación de los proveedores de contenidos y servicios en internet; nombres de dominio, protección jurídica del *software*, comercio electrónico, contratos electrónicos, sistemas expertos, teletrabajo, entre otras[103].

En el Externado cuentan con una *especialización* (de un año) y una *maestría* (de dos años) en Derecho Informático y de las Nuevas Tecnologías, que exploran en profundidad las nuevas tecnologías, su aplicación al ejercicio del derecho; Gobierno y Administración Electrónica incluye dos materias de Protección de los Datos Personales, Protección Jurídica

[101] Curso Pontificia Universidad Javeriana de Protección de Datos Personales en la Era Digital, https://www.edx.org/es/course/proteccion-de-datos-personales-en-la-era-digital.

[102] Diplomado Pontificia Universidad Javeriana como Auditor Interno en Sistemas de Gestión de la Seguridad de la Información ISO 27001:2013, https://www.javeriana.edu.co/documents/16817/10399257/D_Ciberseguridad.pdf/00d1e94e-374f-4386-bfad-172936c1647f

[103] Intensificación en Derecho Informático, Universidad Externado de Colombia, https://www.uexternado.edu.co/derecho/intensificaciones-en-derecho-informatico/.

del *Software*, Propiedades Incorporales en el Ciberespacio, Seguridad de los Sistemas de Información y Documento Electrónico, Firma Digital, Contratos de Nuevas Tecnologías, Servicios de la Sociedad de la Información, y Comercio Electrónico y Delitos Informáticos. Evidentemente, un abogado con estas competencias está en capacidad de dar a sus clientes todas las garantías exigibles relativas al deber de secreto y de desempeñarse además en el área de Legal Tech. Aunque muy útiles, no todos estos conocimientos pueden incorporarse en los programas de pregrado; pero un mínimo de comprensión sobre los ciberriesgos y las obligaciones en materia de protección de datos sí son exigibles a cualquier abogado. La maestría en Gestión del Riesgo incluye entre sus áreas de formación específica: Riesgo Reputacional, Gestión de Riesgo Legal y Contractual, Riesgo Operativo y Continuidad de Negocio y una de sus cinco áreas de desarrollo investigativo es la de Riesgos Informáticos y Nuevas Tecnologías. En otros estudios de posgrado, por ejemplo, en su Especialización de Inspección, Vigilancia y Control se incluyen dos materias (suman 48 h) de Tecnologías (suman 48 h), que pretenden desarrollar competencias en la aplicación de nuevas tecnologías a los procesos de supervisión. En esta misma universidad se ofrece una especialización en Regulación y Gestión en TIC, Telecomunicaciones y Ecosistema Digital, una de cuyas doce asignaturas es Propiedad Intelectual, Derechos de Autor y Protección de Datos. No se encuentra una asignatura específica de ciberseguridad y hay un curso de Ciberseguridad Empresarial: Diseño de Perfiles y Cargos[104] (de 20 h).

La Facultad de Jurisprudencia de la Universidad del Rosario cuenta con veintiún especializaciones, nueve maestrías y numerosos cursos de educación continua. No se imparten asignaturas troncales relativas a ciberseguridad y protección de datos personales en estudios de pregrado. Su escuela de verano incluye el curso Ejercicio del Derecho en la Era Digital[105]. También ofrece el *Legal Tech Intensive Course*[106], una serie

[104] Curso de Ciberseguridad Empresarial, Diseño de Perfiles y Cargos Universidad Externado de Colombia, https://www.uexternado.edu.co/programa/administracion-de-empresas/curso-ciberseguridad-empresarial-diseno-de-perfiles-y-cargos/.

[105] Curso sobre el Ejercicio del Derecho en la Era Digital, Universidad del Rosario, https://www.urosario.edu.co/summer-school/Cursos/el-ejercicio-del-derecho-en-la-era-digital-1/.

[106] Legaltech Intensive Course, Universidad del Rosario, https://www.urosario.edu.co/Eventos-UR/Facultad-de-Jurisprudencia/Legaltech-Intensive-Course/.

de seminarios web que brinda conocimientos y herramientas útiles para desarrollar la virtualización de todo tipo de documentos y operaciones, entre los que se incluye uno específico de "Legaltech x Data Protection".

En la Universidad Nacional no se incluye ninguna materia de ciberseguridad, protección de datos, derecho y tecnología o protección de la privacidad en los estudios de pregrado de Jurisprudencia o Derecho. A pesar de que existe un amplio catálogo de estudios de posgrado en Derecho, compuesto por doce especializaciones y cuatro maestrías, entre los que se desarrollan más de 250 seminarios optativos, no se incluye ninguna asignatura o seminario enfocado en la ciberseguridad y la protección de datos personales. El diplomado de Start Ups y Emprendimiento incluye tres horas de *habeas data* (Importancia del tratamiento de datos personales, Desarrollo de la política de privacidad, Manejo e implementación de la política en las diferentes áreas de la empresa). La Universidad Nacional ofrece una línea de formación en ciberseguridad que consta de cuatro cursos, a saber: Introducción a la Ciberseguridad (de 15 h), *Cybersecurity Essentials* (de 30 h), *Network Security*[107] (de 72 h) y *CiberOps Associate*[108] (de 72 h), pero no está orientado a profesionales del Derecho, puesto que los prerrequisitos son específicos del área de informática[109].

En la Universidad de La Sabana, los estudiantes de Derecho cuentan con ocho líneas de intensificación, cuatro maestrías y seis especializaciones, en las que no se contemplan materias específicas de ciberseguridad y protección de datos. Tampoco se incluyen en los programas de Unisabana *E-learning* o de Educación Continuada. Ofrecen un curso intersemestral de Humanismo Digital, Ética y Tecnología, Humanización Tecnológica, Inteligencia Artificial[110] que aborda el tema de la protección de datos.

[107] Curso de *Network Security*, Universidad Nacional de Colombia, http://catc.unal.edu.co/cursos/seguridad/network-security.

[108] Curso de Cyberops, Universidad Nacional de Colombia, http://catc.unal.edu.co/cursos/seguridad/cyberops.

[109] Programa de Pregrado en Derecho, Universidad Nacional de Colombia, http://derecho.bogota.unal.edu.co/formacion/pregrado/ciencia-politica/informacion-del-programa/.

[110] Programa de Humanismo Digital Universidad de la Sabana, https://www.unisabana.edu.co/intersemestrales/portafolio-de-cursosfacultad-de-derecho-y-ciencias-politicas/humanismo-digital/.

No se han considerado los programas de doctorado de estas universidades puesto que las líneas de investigación varían con el tiempo y podrían caber los temas de ciberseguridad y protección de datos entre los temas aceptados por los investigadores que dirigen las tesis en curso.

La academia desempeña un papel esencial en Colombia en referencia a protección de datos, privacidad, seguridad de la información y ciberseguridad, través de las publicaciones y eventos de sus centros especializados en la investigación, análisis y difusión de la materia, entre los que se destacan el Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI)[111] de la Universidad de los Andes; el Observatorio Ciro Angarita Barón de Protección de Datos Personales de la misma institución; el Centro de Investigación de Derecho Informático (CIDI) del Externado de Colombia y el Observatorio de Ciberseguridad y Delito Informático iURiscyber de la Universidad del Rosario. Su labor de investigación y concienciación es esencial para impulsar la protección del derecho a la privacidad en el entorno de la abogacía y profesiones afines. Su colaboración con investigadores y profesionales de otros países y con entidades como la SIC (máxima autoridad en materia de protección de datos personales en Colombia) o la Red Iberoamericana de Protección de Datos Personales permite (por medio de publicaciones, jornadas, congresos y difusión de buenas prácticas) dar a conocer estos temas que no se incluyen en el plan de estudios, a la vez que contribuye a promover el análisis de riesgos para los derechos y libertades de las personas, a desarrollar el conocimiento y la propia legislación que los cobija.

Sin embargo, a pesar de su existencia, estas competencias no se abordan en las materias troncales de pregrado, aun cuando, en cualquier rama en la que quieran desempeñarse, deban implementar medidas técnicas y organizativas eficientes para preservar la privacidad de los datos que traten en razón de su ejercicio. A la fecha, no existe un examen o requisito relativo a las competencias en ciberseguridad y protección de datos para colegiarse como abogado.

[111] Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI), Universidad de los Andes, https://gecti.uniandes.edu.co/.

Es esencial incluir contenidos de ciberseguridad y protección de datos personales en los pregrados de Derecho por la relación directa de estas materias con el *compliance* por parte de los abogados y por la propia viabilidad y continuidad de negocio de los despachos donde se desempeñen como empleados o profesionales liberales. Este tipo de cambios suele llevar su tiempo, pero el avance imparable de las amenazas a los propios abogados y sus representados por la vía de la seguridad de la información y las exigencias legales en materia de protección de datos no da tregua a negociaciones interminables. La academia tiene que dar un paso adelante para solucionar esta compleja situación, sin olvidar que, con relación a la profesión de abogado, es al Ministerio de Justicia al que le corresponde "auspiciar, en colaboración con universidades e institutos oficiales y privados la formación especializada de los abogados y la programación de cursos de actualización de conocimientos"[112], así como "procurar la colaboración de las facultades de Derecho y de los abogados con el Gobierno y el Congreso en la actualización de normas y con la Administración de Justicia en la tecnificación de su trabajo y en el avance de la doctrina"[113].

La existencia de programas como la intensificación de derecho informático, o demás cursos aquí contemplados, es muy valorable, pero no garantiza la concienciación y transformación a corto plazo que requiere el sector de la abogacía para brindar a sus clientes las garantías exigibles en materia de seguridad de la información.

Se requiere un pacto entre el Ministerio de Justicia, las facultades de Derecho y el Colegio Profesional de Abogados de Colombia para que todos los nuevos profesionales entiendan que el secreto profesional no depende exclusivamente de su buena voluntad y la de su equipo, sino que en este mundo interconectado en el que desempeñarán su actividad deberán actuar bajo el principio de *accountability*, asumiendo el costo de cumplir con la normativa vigente en materia de protección de datos personales y poder demostrarlo.

Asimismo, se deben formular soluciones conjuntas para solventar la situación de los profesionales en ejercicio que no contaron con esta

[112] Decreto 196 de 1971, de 12 de febrero de 1971, por el cual se dicta el Estatuto del Ejercicio de la Abogacía, art. 44.7.

[113] *Ibid*., art. 44.12.

concienciación y formación durante su paso por la universidad, y que tienen que demostrar su responsabilidad proactiva frente a la protección de datos personales y demás información confidencial proporcionada por sus clientes.

Este nuevo escenario, que configura las competencias en seguridad de la información y protección de datos personales como transversales en todas las áreas del derecho, abre la puerta a un *gran pacto del sector legal por la seguridad de la información y la protección de datos de carácter personal*. La academia ya ha dado el primer paso creando centros de investigación y fomentando cursos de formación continua, especializaciones o maestrías. Es tiempo de dar otro paso decisivo liderando el proceso de concienciación de los responsables del Ministerio de Justicia y del Colegio Profesional de Abogados, puesto que la ciberdelincuencia y la normativa en protección de datos personales vigente en Colombia —que, influenciada por el RGPD, sin duda tenderá a ser más exigente en términos de responsabilidad activa y de procedimientos sancionadores— hacen de los abogados un colectivo muy vulnerable, que a su vez deja en situación de vulnerabilidad a sus clientes, colaboradores y empleados. La misión de los abogados está en entredicho hasta tanto puedan asegurar la confianza de sus clientes, la integridad, confidencialidad y disponibilidad de la información que gestionan y la continuidad de su propio negocio.

Análisis dafo del ejercicio de la abogacía a la luz de las exigencias de la normativa en protección de datos personales

D	A
• Los despachos pequeños no cuentan con personal interno del área TI especializado en seguridad de la información. • Escasa conciencia del riesgo en seguridad de la información. • Escasa comprensión de la normativa vigente en protección de datos personales y ciberseguridad y sus implicaciones en la profesión. • La mayoría de los abogados en ejercicio no recibieron formación en nuevas tecnologías durante su carrera y tampoco entienden la necesidad de cubrir ese déficit como un imperativo para el ejercicio de su profesión. • Ausencia o deficiencia de medidas técnicas y organizativas suficientes para garantizar la confidencialidad, disponibilidad e integridad de los datos personales y otra información confidencial de cuyo tratamiento son responsables o encargados. • Profesionales de prestigio en diversas ramas (penal, civil, mercantil, internacional) graduados antes de la aparición de Facebook y demás redes sociales en muchos casos no son miembros activos de estas (baja presencia y participación). Esta incomprensión de su funcionamiento práctico les dificulta el análisis de riesgos y la interpretación de denuncias apoyadas en progresos tecnológicos. • Obligación de cifrar por parte de cualquier abogado en el ejercicio de su profesión, respecto del fichero de clientes desconocida o mal interpretada por muchos profesionales de la rama legal.	• Crecimiento del negocio de cibercrimen viene acompañado de sofisticación. Elevada dificultad de los abogados para identificar amenazas y fugas de información por sí mismos en el plazo legalmente exigible por el RGPD (72 horas). • Obligación de notificar brechas ante autoridades de control no implica multas, pero obliga a demostrar cumplimiento (sin tiempo de reacción). Muchos abogados hoy no están preparados. Posibles sanciones que ponen en jaque la continuidad de su negocio. • Obligación de notificar a los afectados cuando la fuga de información entrañe un riesgo para sus derechos y libertades (72 h en el RGPD). Pérdida de credibilidad del abogado que pone en jaque la continuidad de su despacho. • Ataques basados en ingeniería social (suplantación de un socio del despacho, de un cliente o un colaborador). • Incidentes de fuga de información pueden terminar en difusión, publicación o uso ilegítimo de datos de carácter personal de cuyo tratamiento el abogado sea responsable, corresponsable o encargado. • Empleados o socios descontentos que actúen como adversarios internos revelando información a terceros (incluso a la competencia o a la contraparte de un caso). • *Crackers* que roben información confidencial para chantajear al despacho o venderla al mejor postor.

F	O
• ¿Qué tipo de abogados o despachos puede aportar valor a sus clientes brindando garantías de seguridad de la información que gestionan? • Profesionales formados en análisis de riesgos. • Profesionales que hayan completado su formación en Derecho con cursos de Educación Continuada en protección de datos personales, *compliance* y ciberseguridad. • Despachos que cuenten con ingenieros informáticos y especialistas en derecho de protección de datos que aporten un necesario enfoque interdisciplinario al análisis de riesgos cuando ejerzan funciones asimilables a las del delegado de protección de datos.	• Modificar el pénsum académico de la carrera de Derecho considerando profundizar en temas de nuevas tecnologías e implicaciones para la profesión. • Promover la doble titulación en Derecho y Tecnología. • Promover la maestría en Derecho Tecnológico con una visión netamente práctica. • Externalizar los riesgos conscientemente asumidos como aceptables por medio de pólizas de seguros de ciberseguridad y/o protección de datos, o al menos ampliar las coberturas de los seguros de responsabilidad civil con estas coberturas. • Promover una cibercertificación para abogados, que si bien no tendrá la cantidad de controles que puede tener una ISO 27001, o el nivel de profundidad en conocimientos de la norma que pide la certificación de DPD promovido por la AEPD, pueda dar unas garantías mediante un esquema certificador como el de los *cyber essentials*[114] en el Reino Unido, o el "Common Sense Framework"[115], basado en un examen de conocimientos y una auditoría de medidas técnicas, procedimentales y documentales determinadas como las mínimas exigibles.

Fuente: Elaboración propia.

[114] "Cyber Essentials", United Kingdom National Cyber Security Centre, https://www.ncsc.gov.uk/cyberessentials/overview.

[115] "Home", Common Sense Security Framework (CSSF), https://commonsense-framework.org/.

Conclusiones

No cabe duda de que el progreso tecnológico, la ingente cantidad de información que circula en internet, la generalización de redes sociales y aplicaciones informáticas de todo tipo a nivel global, las nuevas exigencias legales y el lucro que proporciona el cibercrimen imponen a la abogacía un reto sin precedentes para el cumplimiento de la misión de defender los derechos de la sociedad y los particulares con los recursos de que disponen los despachos hoy en día.

La reforma de los pénsums de Derecho no puede hacerse esperar. Es imprescindible crear conciencia acerca de los riesgos para la seguridad de la información propios de los tratamientos de datos personales y secretos empresariales de la profesión de la abogacía antes de que los nuevos profesionales se titulen, puesto que una inadecuada gestión de los activos de información que desemboque en una fuga de información del despacho no solo pone en riesgo la continuidad de este ante la amenaza de sanciones pecuniarias o administrativas y del nefasto impacto en la reputación de la firma y del profesional, sino que implica un ilícito deontológico y puede configurar un delito.

La ciberseguridad y la protección de datos personales son parte esencial del *compliance* y su cumplimiento no puede depender de cursos voluntarios en los que se matricule anualmente un puñado de los cientos de abogados graduados en las facultades de Derecho acreditadas a lo largo y ancho del país. La abogacía se ha transformado a lo largo de los siglos en un servicio de la sociedad, y en medio de la revolución tecnológica y de las comunicaciones más importante y rápida de la historia no puede mirar hacia un lado. Los nuevos profesionales deben estar preparados para enfrentarse exitosamente a las nuevas tecnologías, entender sus implicaciones para los clientes y para el propio funcionamiento del despacho y llevar a cabo un análisis de riesgos de su actividad, tal como exige de ellos el nuevo marco normativo internacional.

Para aquellos abogados que ya culminaron estos estudios y hoy ejercen sus funciones como empleados o profesionales liberales resultan exigibles los cursos de actualización que puedan asegurar a la empresa o cliente particular que les entrega su información confidencial (comprometiendo su privacidad, dignidad y/o patrimonio), que está preparado para gestionarla con seguridad.

Cabe plantearse la creación de algún tipo de cibercertificación para abogados, que demuestre que se cuenta con las medidas técnicas y organizativas exigibles para proporcionar dichas garantías. Esto, obviamente, requiere un periodo de transición, pero a pesar de la inversión económica y temporal que demanda, no puede ser tan amplio, en la medida en que los riesgos para los derechos y libertades de los clientes crecen cada día y el riesgo para la supervivencia de los despachos también.

El *compliance* y la ciberseguridad requieren presupuesto para ejecutar un plan de acción paulatino y continuado que implica inversiones en tecnología, formación y concienciación continuada, ciberejercicios, auditorías internas y externas para evaluar si las medidas que se han tomado son efectivas y priorizar las siguientes. En caso de un ciberincidente que ocasione una brecha de información en un despacho de abogados, puede haber serias consecuencias para la reputación, la cuenta de resultados y la continuidad de negocio si no se demuestra que se han tomado medidas para evitarlo, de conformidad con los recursos de la empresa, sus riesgos y las soluciones disponibles en el mercado. Lo que no puede sostenerse frente a una autoridad de protección de datos ni frente a un juez, en ninguna empresa y menos aún en un despacho de abogados, es haber repartido beneficios y no haber destinado recursos a proteger los activos de información, cifrar los ficheros de clientes y tomar las medidas apropiadas para mitigar los riesgos propios de la actividad que ejercen, o al menos demostrar que tienen un plan coherente que ya han empezado a implementar.

De la misma manera que la prevención de riesgos laborales no se cubre entregando una vez equipos de protección individual a los trabajadores en riesgo, la protección de datos personales no se puede dar por sentada con unos contratos que se firmaron meses o años atrás y unas medidas implementadas en ese entonces con asesoramiento externo o interno. Los abogados a cargo del *compliance* tienen el reto de comprometer a las juntas directivas con la ciberseguridad, como parte estratégica de este,

> […] cuidando el alcance y contenido de los controles que llevan a cabo, dado que asume riesgos tan significativos como querellas criminales por descubrimiento de secretos y vulneración de la intimidad de otros hasta importantes sanciones para la empresa por vulneración de la protección

de datos de carácter personal (determinación de perfiles, acceso a información sensible, etc.)[116].

Lo que persiguen las autoridades de protección de datos no es una lista de verificación de cumplimiento de medidas prestablecidas, sino evidenciar un plan de acción a corto, medio y largo plazo, coherente con un análisis de riesgo pormenorizado de la actividad, que se ajuste a la idiosincrasia del despacho, sus recursos humanos y financieros. No es una foto estupenda del día de la inspección, sino un video del trabajo previo y un buen guion del posterior.

Así como existen hoy en día estrictas normativas respecto a la insonorización de locales dedicados a bares y discotecas; la adaptación de los servicios y rampas que faciliten la accesibilidad a personas discapacitadas, o son exigibles condiciones altísimas a nivel sanitario que obligatoriamente deben asumir los empresarios de los respectivos sectores o profesionales de la salud, la indomable evolución del cibercrimen nos impone reformas organizativas, técnicas y formativas que pueden parecer inasumibles, pero que dejan de serlo cuando lo que está en juego es precisamente un derecho fundamental como lo es la protección de datos personales. Al fin y al cabo, lo que se protege desde el nuevo paradigma normativo en torno a este derecho no son los datos sino la libertad, dignidad, privacidad y el derecho a la individualidad de cada uno de nosotros y de nuestros seres queridos. Para ello, el RGPD, o las distintas normativas que de este se deriven, no debe ser asumido por los abogados como una meta, sino como un camino.

La proliferación de leyes de privacidad, protección de datos y ciberseguridad en todo el mundo, inspiradas en el RGPD, hace altamente difícil y casi improbable para las multinacionales aplicar estándares de cumplimiento diferentes para un mismo propósito. Queda clara la necesidad de universalizar las garantías exigibles para permitir flujos internacionales de información indispensables para el crecimiento sostenible del comercio internacional. Nuestra propuesta sería establecer un único estándar normativo internacional por la vía de un acuerdo multilateral en materia de protección de datos personales, cuyo máximo garante sea

[116] Jesús Rafael Mercader Uguina, "El régimen laboral del *compliance officer*: Un camino por andar", en *Trabajo y Derecho: Sección Práctica Jurídica y Despachos Profesionales* (Wolters Kluwer, 2018), 5.

la Organización Mundial del Comercio (OMC). Sin duda, habrá reticencias, particularmente entre los defensores del neoliberalismo, la mano invisible y el principio de mínima intervención de los mercados, pero probablemente las multinacionales de la economía del dato que más hicieron *lobby* para impedirlo sean las más interesadas en promoverlo. Habrá reticencias sin duda por parte de algunos gobiernos, pero podría recurrirse a una solución intermedia que consiste en un escudo de privacidad impulsado por la OMC al que puedan adherirse voluntariamente las empresas de todo el mundo dispuestas a respetar la libertad y los derechos de las personas. En la medida en que crezca la conciencia de los usuarios en los seis continentes, la presión de los propios consumidores hará el resto.

Bibliografía

Abanlex. *Primer informe sobre la obligación legal de cifrar información y datos personales*. Madrid: Sophos, 2014.

Agencia Española de Protección de Datos (AEPD). *Guía de privacidad desde el diseño*. AEPD, 2019. https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

— *Guía de protección de datos por defecto*. 2020. https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf

— *Guía para la notificación de brechas de datos personales*. AEPD, 2021. https://www.aepd.es/es/documento/guia-brechas-seguridad.pdf

— *Informe del Gabinete Jurídico n.º 0494/2009. Necesidad de cifrado de datos para la comunicación de datos especialmente protegidos*. AEPD, 2009.

Agencia Española de Protección de Datos (AEPD), Autoridad Catalana de Protección de Datos (APDCAT) y Agencia Vasca de Protección de Datos. *Directrices para la elaboración de contratos entre responsables y encargados del tratamiento*. Madrid: 2017.

Alonso Lecuit, Javier. http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari23-2018-alonsolecuit-reglamento-general-proteccion-datos.

Álvarez-Sala Walther, Juan José. "La actuación notarial: Entre la privacidad y la transparencia". *El Notario del Siglo XXI*, n.º 81 (octubre del 2018). Publicación electrónica. http://www.elnotario.es/hemeroteca/revista-81/

academia-matritense-del-notariado/8905-la-actuacion-notarial-entre-la-privacidad-y-la-transparencia.

American Bar Association (ABA). *ABA Techreport 2019: Cybersecurity.* 16 de octubre del 2019. https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cybersecurity2019/

"Big data, small politics: Can the EU become another AI superpower?". *The Economist*, 20 de septiembre del 2018.

Brand, Carlos. "'Empresarios invierten 190 000 millones al año para evitar el cibercrimen': Declaraciones del Sr. Jay García, arquitecto de la firma Controles Empresariales". *RCN Radio*, 1.º de julio del 2019. https://www.rcnradio.com/tecnologia/empresarios-invierten-190-mil-millones-al-ano-para-evitar-el-cibercrimen.

Broadwell, Martin. "Teaching For Learning (XVI)". *The Gospel Guardian* 20, n.º 41 (1969): 1-3. http://www.wordsfitlyspoken.org/gospel_guardian/v20/v20n41p1-3a.html

Buontempo, Christopher J. y Cynthia Larose. "US state Privacy Law Check-In-Update". Mintz. https://www.mintz.com/insights-center/viewpoints/2826/2021-04-30-us-state-privacy-law-check-update.

Cano, Jeimy. "The human factor in information security: The weakest link or the most fatigued?". *ISACA Journal*, n.º 5, 2019.

Cassens Weiss, Debra. "Jones Day is hit by vendor data breach; hackers post files they claim were stolen from the law firm". *ABA Journal*, 17 de febrero del 2021. https://www.abajournal.com/news/article/jones-day-is-hit-by-vendor-data-breach-hackers-post-files-they-claim-were-stolen-from-the-law-firm.

— "More than 100 law firms have reported data breaches; two big law firms affected". *ABA Journal*, 18 de octubre del 2019. https://www.abajournal.com/news/article/more-than-100-law-firms-have-reported-data-breaches-2-biglaw-firms-affected.

Colegio Notarial de Madrid. "Un derecho fundamental de difícil protección". *El Notario del Siglo XXI*, n.º 81 (septiembre-octubre del 2018). Publicación electrónica. http://www.elnotario.es/hemeroteca/revista-81/editorial/8921-un-derecho-fundamental-de-dificil-proteccion.

Consejo General de la Abogacía Española y Agencia Española de Protección de Datos (AEPD). "Utilización del *cloud computing* por los despachos de abogados y el derecho a la protección de datos de carácter personal". 2012.

Consejo General de la Abogacía Española, Instituto de Ciberseguridad de España (Incibe) y Agencia Española de Protección de Datos (AEPD). *Cómo*

gestionar una fuga de información en un despacho de abogados. Madrid: E-Book-Guías TIC, 2016.

Cremades López de Teruel, Fernando Javier. "La nueva Ley Orgánica de Protección de Datos y el poder judicial: Un juego de mercaderes en el templo del reglamento general de la Unión Europea". *La Ley*, n.º 9430, 6 de junio del 2019.

"Cyber essentials". *United Kingdom National Cyber Security Centre.* https://www.ncsc.gov.uk/cyberessentials/overview.

Davis, James M. y Bradley Dlatt. "How to prepare yourself and your clients to respond to data breaches". *ABA Journal*, 19 de septiembre del 2019.

Decreto 196 de 1971, de 12 de febrero de 1971, por el cual se dicta el Estatuto del Ejercicio de la Abogacía.

Decreto 1377 del 2013, 27 de junio del 2013, por el cual se reglamenta parcialmente la Ley 1581 del 2012, *Diario Oficial* 48834.

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio del 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Fernández Hernández, Carlos. "El RGPD ¿Última oportunidad para salvaguardar nuestros datos personales?". *Actualidad Civil*, n.º 5 (2018): 4. Publicación electrónica. https://dialnet.unirioja.es/servlet/articulo?codigo=6437477.

García González, Aristeo, Claudio Ragni Varga, Claudio Roberto Santos, Cynthia Téllez Gutiérrez, Daniel López Carballo, Dulcemaría Martínez Ruíz, Edgar David Oliva Terán, Francisco Ramón González-Calero Manzanares, Héctor E. Guzmán Rodríguez, Javier Villegas Flores, João Ferreira Pinto, Jorge Augusto Tena Ramírez, Jorge Luís García Obregón, José Luís Colom Planas, Laura Vivet Tañà, Marta Sánchez Valdeón, Matilde Susana Martínez, Romina Florencia Cabrera, Ruth Benito Martín, Salvador Serrano Fernández y Wilson Rafael Ríos Ruiz. "Protección de datos y *habeas data*: Una visión desde Iberoamérica". *XVIII Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos*. Coordinada por Daniel López Carballo y Francisco Ramón González-Calero Manzanares (coordinador adjunto). Madrid: AEPD, *Boletín Oficial del Estado*, 2015.

García Mahamut, Rosario. "El derecho fundamental a la protección de datos: El Reglamento 2016/679 como elemento definidor del contenido esencial del artículo 18.4 de la Constitución". *Anuario de Derecho Parlamentario*, n.º extra 31 (2018): 59-80.

"GDPR+1 year: Business struggles with data privacy regulations increasing". *Thomson Reuters*. http://ask.legalsolutions.thomsonreuters.info/GDPR1YearBusinessStrugglesReport.

Gil, Elena. "*Big data*, privacidad y protección de datos". *XIX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos*. Madrid: Agencia Española de Protección de Datos, Boletín Oficial del Estado, 2015.

Herrán Ortiz, Ana Isabel. "Aproximación al derecho de protección de datos en Europa: El RGPD a debate". *Derecho, Empresa y Sociedad,* n.º 8 (2016): 179-200.

"Home". Common Sense Security Framework. https://commonsenseframework.org/

Hughes, Sarah Jane. "Did the National Security Agency destroy the prospects for confidentiality and privilege when lawyers store clients' files in the cloud and what, if anything, can lawyers and law firms realistically do in response?". *Articles by Maurer Faculty*, n.º 1342 (2014): 404-435.

Instituto de Ciberseguridad de España (Incibe). *Dispositivos móviles personales para uso profesional (BYOD): Una guía de aproximación para el empresario*. 2017. https://www.incibe.es/protege-tu-empresa/guias/dispositivos-moviles-personales-uso-profesional-byod-guia-aproximacion-el.

— *Ganar en competitividad cumpliendo el RGPD: Una guía de aproximación para el empresari*o. 2018. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-ganar-competitividad-cumpliendo-rgpd-metad.pdf.

Jove Villares, Daniel. "Las facultades de control de la información personal en el RGPD". En *Derecho, gobernanza e innovación: Dilemas jurídicos de la contemporaneidad en perspectiva transdisciplinar*", coordinado por Maria Manuela Magalhães, Rubén Miranda Gonçalves y Fábio da Silva Veiga, 363-380. Universidade Portucalense: 2017.

Kang, Cecilia. "Congress moves to overturn Obama-era online privacy rules". *The New York Times*, 28 de marzo del 2017. https://www.nytimes.com/2017/03/28/technology/congress-votes-to-overturn-obama-era-online-privacy-rules.html?smid=tw-nytimes&smtyp=cur.

"Law Firm Cybersecurity Score Card 2019". *LogicForce*, 2019. https://www.logicforce.com/2019/10/07/cyber-security-scorecard-q4-2019/.

Ley 1123 del 2007, 22 de enero del 2007, por la cual se establece el código disciplinario del abogado. *Diario Oficial* 46519.

Ley 1266 del 2008, 31 de diciembre del 2008, por la cual se dictan las disposiciones generales del *habeas data* y se regula el manejo de la información

contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. *Diario Oficial* 47219.

Ley 1273 del 2009, 5 de enero del 2009, por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado —denominado "de la protección de la información y de los datos"— y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. *Diario Oficial* 47223.

Ley 1581 del 2012, 18 de octubre del 2012, por la cual se dictan disposiciones generales para la protección de datos personales. *Diario Oficial* 48587.

Ley Orgánica 3 del 2018, 5 de diciembre del 2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD). *Boletín Oficial del Estado* 294 (2018).

López Aguilar, Juan Fernando. "La protección de datos personales en la más reciente jurisprudencia del TJUE: Los derechos de la CDFUE como parámetro de validez del derecho europeo y su impacto en la relación trasatlántica UE-EEUU". *Teoría y Realidad Constitucional*, n.º 39 (2017): 557-581.

López Calvo, José *et al*. "La adaptación al nuevo marco de protección de datos tras el RGPD y la *LOPDGDD*". Hospitalet de Llobregat: Bosch Wolters Kluwer, 2019.

Marcos Ayjón, Miguel. "Las múltiples implicaciones de la protección de datos en la justicia penal". *La Ley Penal*, n.º 132 (junio del 2018).

Martínez López-Sáez, Mónica. "Una reflexión del derecho fundamental a la protección de datos de carácter personal". Valencia: Tirant Lo Blanch, 2018.

Mayor Gómez, Roberto. "Principales novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales". *Gabilex*, n.º 16 (diciembre del 2018): 14-55.

Mercader Uguina, Jesús Rafael. "El régimen laboral del *compliance officer*: Un camino por andar". *Trabajo y Derecho* (2018).

Organization of American States, Secretariat for Legal Affairs. "Data protection". http://www.oas.org/dil/data_protection_privacy_habeas_data.htm.

Ortega Jiménez, Alfonso y Juan José Gonzalo Domenech. "Nuevo marco jurídico en materia de protección de datos de carácter personal de la Unión Europea". *Revista de la Facultad de Derecho*. *Universidad de la República de Uruguay*, n.º 44 (2018): 93.

Pacheco Cifuentes, Alfonso. "El abogado ante el deber de información a sus clientes y el nuevo Reglamento General de Protección de Datos". *La Ley*, n.º 8804 (15 de julio del 2016).

Padín Vidal, Alejandro. "Protección de datos en Colombia, Perú, México y Brasil: Referencia a Estados Unidos". En *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, editado por José López Calvo *et al*., 1057-1084. Hospitalet de Llobregat: Bosch Wolters Kluwer, 2019.

Painter Randall, Karen y Steven A. Kroll. "Getting serious about law firm cybersecurity". *New Jersey Lawyer* (junio del 2016): 54-58.

"Los principales líderes políticos de 'Los Papeles de Panamá'". *eldiario.es*, 3 de abril del 2016. https://www.eldiario.es/economia/politicos-mundiales-aparecen-papeles-panama_0_501500208.html.

Quacquarelli, Symonds. "Ranking QS 2021 de universidades para estudiar Derecho en América Latina". https://www.topuniversities.com/university-rankings/university-subject-rankings/2021/law-legal-studies.

Rallo, Artemi. "Privacy and freedom". *European Data Protection Law Review* 4, n.º 2 (5 de febrero del 2018): 150-151. https://edpl.lexxion.eu/article/EDPL/2018/2/5.

Reglamento General de Protección de Datos (RGPD). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril del 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). *DOUE* 119, 4 de mayo del 2016, 1-88.

Recio Gayo, Miguel. "Una aproximación a la aplicación del Reglamento (UE) 2016/679 sobre protección de datos (RGPD) al sector de la abogacía y despachos profesionales". *Trabajo y Derecho.* 2018.

Sobowale, Julie. "Six major law firm hacks in recent history". *ABA Journal*, marzo del 2017. http://www.abajournal.com/magazine/article/law_firm_hacking_history.

State of California Department of Justice, Office of The Attorney General. *California Consumer Privacy Act (CCPA)*. https://oag.ca.gov/privacy/ccpa.

Subiza Pérez, Ignacio. "Sobre cómo nos hemos hecho adultos, casi sin darnos cuenta: Nuevo Reglamento Europeo de Protección de Datos". *Actualidad Administrativa*, n.os 7-8 (2018).

Superintendencia de Industria y Comercio. *Guía para la implementación del principio de responsabilidad demostrada*. Bogotá: SIC, 2017. https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf.

Tarr, Madelyn. "Law firm cybersecurity: The state of preventative and remedial regulation governing data breaches in the legal profession". *Duke Law & Technology Review* 15, n.º 1 (2016): 234-252.

Tashea, Jason. "Lawyers are failing at cybersecurity, says *ABA Tech Report 2019*". *ABA Journal,* 24 de octubre del 2019. http://www.abajournal.com/news/article/lawyers-are-failing-at-cybersecurity-says-aba-techreport-2019.

Tidy, Joe. "Hackers hit A-list law firm of Lady Gaga, Drake and Madonna". *BBC News*, 12 de mayo del 2020. https://www.bbc.com/news/technology-52632729.

Tribunal de Justicia de la UE (Gran Sala), Sentencia de 16 de julio del 2020, Asunto C-311/18. Data Protection Commissioner contra Facebook Ireland Ltd. y Maximillian Schrems.

Valderas, Juan J. "Cómo proteger la confidencialidad de información comercial o personal 'delicada' necesaria para la prueba pericial en un litigio". *La Ley*, n.º 8925 (2017).

Capítulo II

El *big data* como tecnología disruptiva en Colombia*

Carolina Herrera Hincapié

> *Sobre la escritura, Platón decía "[…] Este descubrimiento vuestro engendrará el olvido en el espíritu de los que aprenden porque no usarán su memoria; confiarán en los caracteres escritos externos y no se acordarán de sí mismos… serán aburrida compañía con apariencia de sabiduría sin su realidad […]".*
>
> platón, *Fedro*

Introducción

Durante los últimos años ha habido un cambio drástico en el valor de la "información" y en la posibilidad de encontrar en su explotación un uso económico y social. Esto ha traído grandes beneficios en diferentes esferas, como lo son la medicina y la planeación de políticas públicas, pero ha representado a su vez un gran reto frente a su regulación así como a la protección de los generadores de los datos y a su derecho a determinar cómo quieren que sean tratados.

Actualmente, se producen al día alrededor de 500 millones de tuits, se envían 294 billones de correos electrónicos y se crean 4 *petabytes* de datos en Facebook. Se estima que para el 2025 se producirán al día 463 *exabytes* de datos, lo que es equivalente a 212.765.957 DVD por día[1]. Esto

* Para citar este capítulo: http://dx.doi.org/10.15425/2017.573.

[1] Jeff Desjardins, "How much data is generated each day?", *The World Economic Forum,* 17 de abril del 2019, https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/.

nos permite entender de manera general la magnitud de cantidad de información que se produce actualmente, y con esto, la alta relevancia de tener una regulación y cultura apropiadas para aprovechar al máximo los beneficios derivados del procesamiento de esta información por medio del uso de tecnologías, mientras que se garantizan los derechos y el control sobre la información asociada a un individuo en particular.

En este sentido, el presente capítulo tiene dos objetivos: (1) Realizar un análisis jurídico a profundidad sobre los beneficios y riesgos que trae consigo la explotación masiva de la información usando nuevas tecnologías, como el *big data*, a la luz de cómo está regulado en Colombia al día de hoy; y (2) proponer un conjunto de prácticas que les permitan a los titulares de la información[2] establecer unos códigos de conducta que garanticen una sana explotación de sus datos.

Metodología

Para lograr cumplir con el objetivo descrito, se hará una contextualización del concepto de *big data* y su papel como tecnología disruptiva. De esta forma se proseguirá con una exposición del estado actual de la regulación del tratamiento de la información en Colombia, así como de las herramientas que tienen las personas para ejercer este derecho.

Teniendo en cuenta lo anterior, se continuará con un análisis detallado de los beneficios y los riesgos que trae consigo la explotación debida o abusiva del *big data* y los casos en los cuales estos se pueden ver ejemplificados.

Finalmente, se propondrán ciertas prácticas a la mano de los generadores de la información, mediante las cuales podrán garantizar una protección de sus datos y asegurarse de que esta sea tratada de la forma en la que hayan accedido.

[2] L. 1581/2012, art. 3. Persona natural cuyos datos sean objeto de tratamiento.

Big data

Breve contexto histórico: la primera revolución digital

Siguiendo a Klaus Schwab, es posible resumir el desarrollo industrial de la humanidad en cuatro grandes revoluciones. Este autor sostiene que "La palabra *revolución* indica un cambio abrupto y radical. Las revoluciones se han producido a lo largo de la historia cuando nuevas tecnologías y formas novedosas de percibir el mundo desencadenan un cambio profundo en los sistemas económicos y las estructuras sociales"[3]. En el marco de la primera Revolución Industrial, que va desde 1760 hasta 1840, la manufactura británica se movió de los hogares a las fábricas, lo cual marcó el inicio de la organización jerárquica y una gran movilización de personas que se vieron obligadas a migrar desde las áreas rurales a los centros industriales. Esto creó no solo una resistencia al estilo de vida, sino a las obligaciones derivadas de esta nueva estructura altamente jerarquizada.

Durante la segunda Revolución Industrial, desarrollada a finales del siglo XIX y principios del XX, se incluyó dentro de la industria el uso de la electricidad, la producción a gran escala y una nueva red de transporte y comunicaciones que, si bien desplazó el trabajo de algunas personas, a su vez creó nuevas profesiones, como la ingeniería, la banca y la docencia. A partir de esta revolución, se hicieron mucho más notorias las diferencias socioeconómicas y surgió la clase media, lo que requirió de un papel mucho más activo del Gobierno para formular políticas que regularan esta brecha.

Durante la década de 1960 y hasta mediados de la de los noventa, la tercera Revolución Industrial surgió alrededor de la automatización de los procesos de producción, potencializada gracias a las tecnologías de las comunicaciones y de la información. De esta forma, muchos de los empleos que las personas desempeñaban antes pasaron de la manufactura a los servicios. Un claro ejemplo de la disrupción de la tecnología durante esta época se vio en la resistencia a la adopción de cajeros

[3] Klaus Schwab, "The Fourth Industrial Revolution", *The World Economic Forum*, 14 de enero del 2016, https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab.

automáticos en los años setenta, puesto que al principio se pensaba que afectarían considerablemente a los trabajadores de la banca. Lo que en realidad ocurrió fue que, al automatizar este servicio, el número de sucursales bancarias se elevó y los costos de uso del servicio disminuyeron, lo que les permitió a los bancos dirigir sus recursos a temas menos transaccionales y centrarse más en el servicio al cliente[4].

Finalmente, la cuarta Revolución Industrial se está construyendo sobre la tercera, para ser conocida como la primera revolución digital. Esta se caracteriza por incluir todas las tecnologías desarrolladas hasta ahora, ha eliminado las fronteras que existen en lo físico, digital y biológico y producido no un crecimiento lineal, como las tres anteriores, sino exponencial, por medio de la interconexión de todas las esferas en las que los seres humanos nos relacionamos hoy en día. De esta forma, la primera revolución digital está permeando y disrumpiendo en casi todas las industrias del mundo, transformando la totalidad de sistemas de producción, gerencia y regulación[5].

En el desarrollo de esta revolución, no solo se habla de la transformación digital por el uso de medios digitales en diferentes esferas, sino por la posibilidad que tienen las industrias y los gobiernos de acceder y explotar las tecnologías, lo que les permite extraer el valor de la información mediante la inteligencia artificial, el aprendizaje de máquinas o el internet de las cosas, entre otros. Nada de lo anterior sería posible sin la computación en la nube[6], que presta las condiciones para el procesamiento de esta cantidad masiva de información. Sobre la base de la computación en la nube se da la posibilidad de realizar procesos de

[4] Johan Aurik, "La cuarta Revolución Industrial tendrá un efecto disruptivo sobre el empleo, ¿pero, cómo?", *The World Economic Forum*, 30 de enero del 2017, https://es.weforum.org/agenda/2017/01/la-cuarta-revolucion-industrial-tendra-un-efecto-disruptivo-sobre-el-empleo-pero-como.

[5] Schwab, "The Fourth Industrial Revolution".

[6] National Institute of Standards and Technology (NIST), United States Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-145/final. "La computación en la nube es un modelo que permite el acceso ubicuo, conveniente y bajo demanda de red a un conjunto de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que puedan ser rápidamente proveídos con esfuerzos mínimos de administración o interacción con el proveedor de servicios. Este modelo de nube promueve la disponibilidad y se compone de cinco características esenciales, tres modelos de servicios y cuatro modelos de implementación".

analítica de datos, como lo es el *big data*, concepto que se desarrollará a continuación.

Concepto: el oro negro de la era digital

El concepto del *big data* hace referencia a

> […] la forma en la que las organizaciones, incluyendo públicas y privadas, combinan un alto número de centros de datos, análisis estadístico y otro tipo de técnicas de ingeniería de datos para extraer de estos información que no es deducible por sí sola y correlaciones sorpresivas[7].

Durante los últimos años, el volumen de datos recolectados y almacenados por las entidades públicas y privadas ha aumentado dramáticamente, como ya se indicó. Hoy en día hay más dispositivos móviles que personas en el mundo, y se producen más de cien millones de *gigabytes* o ciento veinticinco millones de memorias USB (de ocho *gigabytes* cada una) en un solo día, lo que sería la altura de 4167 edificios como el BD Bacatá[8].

Esta tendencia se ha dado gracias a la reducción de los costos de almacenamiento de la información, su libre transferencia y la capacidad de analizar instantáneamente grandes cantidades de información usando métodos experimentales y simulaciones a gran escala[9]. Esta enorme cantidad de información se produce, a grandes rasgos, a partir de transacciones en línea, correos electrónicos, videos, imágenes, inicios de sesión, búsquedas en la web, registros médicos, redes sociales, registros satelitales y teléfonos celulares, entre otras fuentes. La importancia que ha adquirido este tema obedece al reconocimiento del inmenso valor social y económico de la información, así como a la intención de

[7] Ira Rubinstein, "Big Data: The End of Privacy or a New Beginning?", *International Data Privacy Law* 3, n.º 2 (mayo del 2013): 74-87.

[8] Departamento Nacional de Planeación (DNP), *Documento CONPES 3920. Política de explotación de datos* (Bogotá: Consejo de Política Económica y Social [CONPES 3920], 2017).

[9] Trevor J. Hastia, Robert Tibshirani y Jerome Friedman. *The Elements of Statistical Learning: Data Mining, Inference, and Prediction* (Nueva York: Springer, 2009).

explotar este potencial para convertir un dato en conocimiento para actuar[10]. Investigadores del MIT han demostrado que las compañías que usan procesos de *data-directed decision-making* tienen un crecimiento de 5-6 % en su productividad[11].

A pesar del extraordinario beneficio social del *big data,* dentro del cual se encuentran grandes descubrimientos en las áreas de la medicina, la seguridad y el uso de energía, todo esto debe ser visto teniendo en cuenta el incremento del riesgo con respecto a la información personal. Existe entonces un problema de dos caras. Por un lado, a los individuos no se les debería solicitar que entregaran su información para el beneficio de las grandes compañías a tan poca retribución directa; por otro lado, el interés personal no debería frustrar los beneficios del *big data*[12].

Así, las constantes tensiones entre los diversos agentes hacen aún más retador establecer una normativa que satisfaga las distintas necesidades. En la figura II.1 se ilustra un sencillo ejemplo de la disyuntiva que puede derivarse de las interacciones entre varios sujetos.

Compañías como Microsoft, Google, Facebook, Apple y Amazon —conocidas como los gigantes de la tecnología— tienen en su poder cantidades masivas de información. En la red social de Instagram, por ejemplo, solo entre enero y septiembre del 2017 se cargaron más de dieciocho mil millones de fotos[13]. Por otro lado, Google ofrece una gran cantidad de productos para el uso intensivo de la información, dentro de los cuales está Gmail, el buscador Chrome, YouTube, Google Maps, Google Analytics, Aplicaciones Google, entre otros[14]. Solo en el buscador de Google, entre enero y septiembre del 2017 se realizaron 1,4 billones de búsquedas. Asimismo, compañías como Amazon y Yahoo buscan

[10] Chris Anderson, "The End of Theory: The Data Deluge Makes the Scientific Method Obsolete", *Wired,* 3 de junio del 2017, https://www.wired.com/2008/06/pb-theory/.

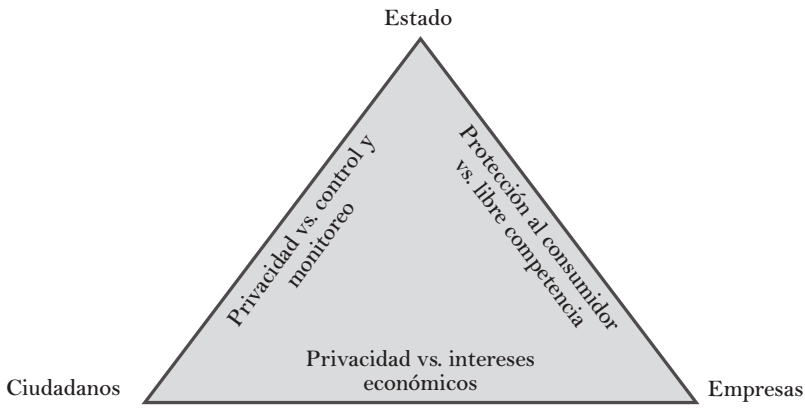
[11] Erik Brynjolfsson, Lorin M. Hitt y Heekyung Hellen Kim, "Strength in Numbers: How Does Data-Driven Decisionmaking Affect Firm Performance?". *SSRN Electronic Journal*, n.º 1 (2011). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819486.

[12] Omer Tene y Jules Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics", *Northwestern Journal of Technology and Intellectual Property* 11, n.º 5 (2012): 244.

[13] DNP, *Documento CONPES 3920*.

[14] Véase http://www.google.com/intl/en/about/products/index.html.

Figura II.1. Tensiones entre partes



Fuente: Elaboración propia.

mejorar sus ingresos valiéndose de la explotación de los millones de datos que recolectan diariamente frente a los perfiles de sus usuarios[15], y empresas como Microsoft y Apple, que desarrollan sistemas operativos y plataformas, reciben igual cantidad de información por medio de sus productos en línea y aplicativos para el celular.

El *big data* como tecnología disruptiva

Para poder entrar a analizar en profundidad las implicaciones del *big data* en el ámbito jurídico, nos parece procedente iniciar por identificar qué factores hacen que una tecnología sea considerada disruptiva.

Las tecnologías disruptivas pueden provenir de cualquier disciplina científica, pero siempre deben compartir cuatro características[16]: (1) un

[15] Nicole Perlrot, "Revamping at Yahoo to Focus on its Media Properties and Customer Data", *The New York Times*, 11 de abril del 2012, http://bit.ly/HUneMM.

[16] James Manyika *et al*., "Disruptive Technologies: Advances that will Transform Life, Business, and the Global Economy", *Mckinsey*, 1.º de mayo del 2013, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/disruptive-technologies.

continuo estado de cambio y desarrollo, (2) permear diferentes esferas sociales, (3) proponer una transformación significativa en el valor y uso de los servicios, y (4) generar un alto impacto económico. A continuación, un breve desarrollo de ellas.

Un continuo estado de cambio y desarrollo

Las tecnologías disruptivas muestran una tendencia a un estado continuo de cambio y de accesibilidad frente a los factores de precio y servicio, mediante la presentación de alternativas y sustituciones a las soluciones que usan las personas en el día a día.

Permear diferentes esferas

Las tecnologías disruptivas deben tener un impacto masivo a nivel económico en diferentes esferas. Así, esta tecnología debe poder afectar la forma habitual de la prestación de un servicio que sirva como plataforma para la interconexión de las industrias y la satisfacción de la demanda en el mercado, o para crear una nueva oferta en este. Una manera de ejemplificar esto es mediante el uso de internet en los teléfonos celulares, lo cual puede llegar a afectar el modo como alrededor de cinco billones de personas experimentan y perciben su vida, dándoles los espacios para innovar y emprender por medio de una plataforma que permita la conexión con los diferentes mercados, consumidores y demanda de forma instantánea.

Proponer una transformación significativa en el valor y uso de los servicios

El valor que genera una tecnología en el mercado debe afectar en gran forma la posición de los servicios que se sustituyen frente a la nueva alternativa, así como el valor al cual estos se coticen en el mercado. Esta característica se percibe por ejemplo en la robótica, por medio de la cual se estima que el impacto potencial en la industria laboral es de 6,3 trillones de dólares; o la tecnología en la nube, que se estima que mejorará

la productividad de la industria generalizada en aproximadamente tres trillones de dólares en gastos en tecnología de la información (TI) mientras que promoverá la creación de nuevos productos y servicios en línea alrededor del mundo, lo cual impactará en los sectores de salud, seguridad y productividad de billones de personas.

Generar un alto impacto económico

Este tipo de tecnologías tienden a tener un impacto dramático en el *statu quo* de la economía y transformar la manera como la gente vive y trabaja. Así, tienen la capacidad de brindar espacios y plataformas que den lugar a nuevas ofertas y, a su vez, permitir a la demanda acceder a ellas de manera más fácil, rápida e instantánea.

Por ejemplo, con la genómica[17] se podrá lograr que los doctores diagnostiquen y traten enfermedades como el cáncer de una forma mucho más eficiente, así se conseguirá aumentar las posibilidades de vida de los pacientes.

Regulación en Colombia

Las técnicas de *big data* no están reguladas expresamente en la legislación colombiana, pero como la materia prima para su desarrollo es la información, especialmente los datos personales, la regulación más importante sobre esta actividad es la que se desprende del derecho al *habeas data*.

Derecho fundamental al *habeas data*

El derecho fundamental[18] al *habeas data* está consagrado en la Constitución Política de Colombia de la siguiente forma:

[17] Rama de la genética que se ocupa del mapeo, la secuenciación y el análisis de las funciones de genomas completos.

[18] "Son fundamentales (i) aquellos derechos respecto de los cuales existe consenso sobre su naturaleza fundamental y (ii) todo derecho constitucional que funcionalmente

> Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas […]

Desde un inicio, en el desarrollo de la jurisprudencia de la Corte Constitucional en Colombia (en adelante, la Corte o Corte Constitucional), este derecho fue interpretado como una forma de garantizar el derecho a la intimidad, por lo que se hablaba de la protección de los datos pertenecientes a la esfera individual en la que los sujetos de derecho pudiesen desarrollar este aspecto de su vida sin intervención del Estado ni de los particulares[19].

Este derecho continuó su desarrollo con una interpretación posterior de la Corte Constitucional, que encontraba una estrecha relación con la manifestación del libre desarrollo de la personalidad, fundamentado en la autodeterminación y libertad que el Estado le otorga al individuo[20]. A partir de 1995 surgió una tercera interpretación por parte de esta corporación, la cual prevalece hasta ahora y reconoce el derecho de *habeas data* como un derecho autónomo cuyo núcleo está compuesto por la autodeterminación informática y la libertad[21]. De esta forma, la sentencia SU-082 de 1995 indicó que el derecho al *habeas data* comprende al menos las siguientes prerrogativas: "a) El derecho a conocer las informaciones que a ella se refieren; b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos; c) El derecho a rectificar las informaciones que no correspondan a la verdad", e incluyó el derecho a la caducidad del dato negativo.

Más adelante, la Corte Constitucional explicó la importancia de diferenciar y delimitar el derecho al *habeas data* frente a otros que pueden llegar a ser relacionados con este, como el derecho al buen nombre

---

esté dirigido a lograr la dignidad humana y sea traducible en un derecho subjetivo." C. Const., Sent. T-361/2014. M.P. Jorge Ignacio Pretelt.

[19] C. Const., Sent. T-414/1992. M.P. Ciro Angarita Barón; T-161 de 1993. M.P. Antonio Barrera Carbonell; y C-913/2010. M.P. Nilson Pinilla Pinilla.

[20] C. Const., Sent. T-340/1993. M.P. Carlos Gaviria Díaz.

[21] C. Const., Sent. SU-082/1995. M.P. Jorge Arango Mejía y T-176/1995. M.P. Eduardo Cifuentes Muñoz.

y a la intimidad. Esta premisa la fundamentó principalmente en tres razones: (1) por ser protegido de forma independiente por vía de tutela, (2) por la delimitación de los contextos materiales de su ámbito de protección, y (3) por las particularidades de su régimen jurídico frente al derecho a la información[22].

Así, la Corte definió el derecho fundamental al *habeas data* como

> […] aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales[23].

Ley estatutaria

En el derecho comparado existen dos modelos de protección de datos mayoritariamente adoptados: un modelo centralizado y uno sectorial.

El modelo centralizado, adoptado en países europeos, parte de una premisa de protección como un derecho humano y una categoría general de datos personales, y de la idea de que cualquier tratamiento de estos es potencialmente problemático y debe sujetarse a unos principios y garantías mínimas que pueden llegar a ser complementadas con regulaciones especiales según el tipo de dato, pero que no suponen una derogación de los estándares generales de protección aplicables tanto al sector público como al privado. En este sistema también es propia la existencia de una entidad central que supervise el cumplimiento normativo y la ejecución de los estándares de protección[24].

Por otro lado, el modelo sectorial, usual en los países con tradición anglosajona, parte de una premisa de protección legal en la cual no hay una categoría común de datos personales, por ende, no se considera que

[22] C. Const., Sent. T-729/2002. M.P. Eduardo Montealegre Lynett.

[23] C. Const., Sent. C-1147/2001. M.P. Manuel José Cepeda Espinosa.

[24] Francesca Bignami, "European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining", *Boston College Law Review* 48, n.º 3 (2007).

todos los datos estén sometidos al mismo tratamiento. En este modelo, se adopta una regulación especial según el tipo de dato que se esté tratando, basada en una ponderación de intereses dependiendo de su relación con el derecho a la intimidad y la defensa nacional, entre otros[25].

En el caso colombiano existen dos leyes estatutarias que regulan el derecho al *habeas data*: la Ley 1266 del 2008 y la Ley 1581 del 2012.

La Ley Estatutaria 1266 del 2008

Tenía el objetivo de fijar los principios generales aplicables a todas las categorías de datos personales, pero a pesar de esta intención de generalidad, solo estableció estándares básicos de protección de datos financieros y comerciales. Como consecuencia de esta reglamentación general, aplicable de forma mínima a todos los datos personales, el legislador adoptó un sistema híbrido entre el modelo centralizado y el sectorial, que se basa en una ley de principios generales y otras regulaciones sectoriales, que están en concordancia con la general pero que atienden la complejidad del tratamiento de los distintos tipos de datos[26]. Así, la Ley Estatutaria 1581 del 2012 busca atender esta complejidad de tratamiento de los datos personales.

A su vez, en cuanto a la normatividad y otras disposiciones que regulan el tratamiento de los datos personales, debe mirarse el Decreto 1377 del 2013 así como el Decreto Único Reglamentario 1074 del 2015, que derogó el anterior.

Ley Estatutaria 1581 del 2012

Como se ha mencionado, esta ley es el marco regulatorio específico para el tratamiento de los datos personales en el país. Además de varias disposiciones frente a las herramientas que tienen las personas para poder ejercer sus derechos, trae consigo una serie de conceptos de altísima

[25] *Ibid*.

[26] C. Const., Sent. C-748/2011. M.P. Jorge Ignacio Pretelt.

importancia, así como los principios rectores del tratamiento de los datos personales.

Según esta ley, un *dato personal* es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables[27]. Así, las personas cuyos datos sean objeto de tratamiento son consideradas los *titulares* de la información. Por su parte, el *tratamiento* se entiende como cualquier operación o conjunto de operaciones sobre datos personales, tales como su recolección, almacenamiento, uso, circulación o supresión. Los datos mencionados se encuentran comúnmente en un conjunto organizado de datos personales objeto de tratamiento conocido como *base de datos.*

De esta forma, la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros decida sobre la base de datos y/o el tratamiento de los datos se considera el *responsable del tratamiento,* quien puede a su vez transmitir esta información a otra persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros y por cuenta del responsable realice el tratamiento de esta. Dicha figura se conoce como el *encargado del tratamiento*.

Principios rectores del tratamiento de datos personales

La Ley Estatutaria también desarrolla los principios rectores del tratamiento de datos personales, los cuales, en virtud del artículo 4 de la mencionada ley, deben aplicarse de manera armónica e integral[28].

A continuación, se hará una descripción de estos principios y se profundizará en aquellos que son más relevantes para el desarrollo del presente trabajo.

[27] Asimismo, esta corporación ha precisado que las características del dato personal son las siguientes: "i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación". C. Const., Sent. T-729/2002. M.P. Eduardo Montealegre Lynett, Ref. Sentencia T-414/1992, M.P. Ciro Angarita Barón.

[28] L. 1581/2012, art. 4.

a. *Principio de legalidad en materia del tratamiento de los datos personales.* Este hace referencia a que el tratamiento es una actividad regulada y sujeta a lo establecido en la ley y demás disposiciones que la desarrollen.
b. *Principio de finalidad.* El tratamiento que se les practique a los datos personales debe obedecer a una finalidad que esté acorde con la Constitución y la ley, y esta a su vez debe ser informada al titular del dato.
c. *Principio de libertad.* Este principio indica que el tratamiento solo puede ser realizado con el consentimiento previo, expreso e informado del titular del dato. De esta forma, los datos personales no pueden ser obtenidos o divulgados sin previa autorización del titular o en ausencia de mandato legal o judicial que releve el consentimiento.

   De esta forma, el ser humano goza del derecho a determinar qué datos desea que sean conocidos. Es por lo anterior que la Corte Constitucional ha reiterado que

> En relación con el carácter previo, la autorización debe ser suministrada en una etapa anterior a la incorporación del dato [...] En relación con el carácter expreso, la autorización debe ser inequívoca, razón por la cual, al contrario de lo sostenido por algunos intervinientes, no es posible aceptarse la existencia, dentro del ordenamiento jurídico colombiano, de un consentimiento tácito. [...] En relación con el carácter informado, el titular no solo debe aceptar el Tratamiento del dato, sino también tiene que estar plenamente consciente de los efectos de su autorización [...][29].

   De acuerdo con el artículo 7 del Decreto 1377 del 2013, esta autorización puede ser obtenida por estas vías: (1) por escrito, (2) de forma oral, o (3) mediante conductas inequívocas del titular que permitan concluir de forma razonable que ella fue otorgada. Estos medios de autorización dispuestos por la ley pueden llegar a chocar con el uso y tratamiento actual de la información, puesto que las personas están compartiendo de forma permanente sus

[29] C. Const., Sent. C-1011/2008. M.P. Jaime Córdoba Triviño.

datos y estos son recolectados para distintos fines sin que siquiera el titular sea consciente de ello, como se verá.

d. *Principio de veracidad o calidad.* La información que esté siendo sujeta a un tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe así el tratamiento que contradiga cualquiera de los anteriores.
   Uno de los mayores retos frente a la regulación de la protección de los datos personales se basa en este principio, puesto que dada la gran cantidad de información que se está compartiendo en todo momento, cuesta llevar un registro claro de esta y, por ende, acudir a los responsables del tratamiento o sus encargados para que realicen esta actualización de la información. Esta problemática se analizará más adelante.
e. *Principio de transparencia*. Hace referencia a la obligación del responsable o el encargado del tratamiento de que, en cualquier momento, dé respuesta sin ninguna restricción acerca de la existencia de los datos que le conciernan al titular.
f. *Principio de acceso y circulación restringida*. El tratamiento únicamente podrán realizarlo las personas naturales o jurídicas autorizadas por el titular, o las indicadas en la ley. De esta forma, los datos personales que no sean considerados información pública[30] no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlado para garantizarlo solo a las personas autorizadas por el titular y la ley.
   Este principio, al igual que el de veracidad o calidad, supone un gran reto para el regulador y para el titular del dato, puesto que una vez que este es compartido por estos medios de divulgación o incluido dentro de una base de datos, es difícil llevar un registro preciso de esta información y de que su uso se ciña a lo inicialmente autorizado.

[30] Los datos serán públicos cuando la ley o la Constitución así lo establezcan, y cuando no sean de aquellos clasificados como semiprivados o privados. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas y los relativos al estado civil de las personas. sic.gov.co/manejo-de-informacion-personal.

g. *Principio de seguridad*. Este principio obliga a que la información sujeta a tratamiento sea manejada con las medidas técnicas, humanas y administrativas necesarias para otorgar un nivel adecuado de seguridad, evitando cualquier tipo de adulteración, pérdida, consulta, acceso o uso no autorizado o fraudulento.
h. *Principio de confidencialidad*. Toda la información que sea tratada y que no tenga la naturaleza de pública deberá a estar sujeta a reserva, incluso después de finalizado su uso.

El presente escrito buscará analizar algunos de los debates más importantes que se dan con relación a los principios descritos y el funcionamiento práctico de tecnologías como el *big data.*

Ámbito de aplicación de la Ley 1581 del 2012

La Ley 1581 del 2012 señala el ámbito de su aplicación en su de la siguiente forma:

> Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada. La presente ley aplicará al Tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. (art. 2)

Así las cosas, para entender más a fondo cómo se protegen los datos de los colombianos, es importante resaltar que el ámbito de aplicación de la Ley 1581 no está sujeto únicamente al territorio del país. De acuerdo con la cita anterior, la ley aplica al tratamiento de datos bien sea en Colombia o en el extranjero, y la normatividad será aplicable de acuerdo con los tratados y convenios internacionales suscritos entre los países (Concepto SIC 16-075042-00003-0000).

Para entender mejor la premisa anterior, es importante ahondar en los conceptos de *responsable* y *encargado* de la información, los cuales son definidos en este mismo orden en el artículo 3 de la mencionada

ley como: "i) Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos; y ii) Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento" (Ley 1581 del 2012). Estos términos son desarrollados y utilizados después por toda la regulación sobre la materia en Colombia. Así, sirven de base para la estructuración de las demás políticas relacionadas con el ámbito de aplicación de la normativa de protección de datos personales en el país.

Decreto Único Reglamentario del Sector de Comercio, Industria y Turismo

El Decreto Único Reglamentario del Sector de Comercio, Industria y Turismo, dentro de varios temas, regula la transferencia y transmisión de datos personales al extranjero. La SIC define estos dos conceptos de la siguiente forma, basándose en el artículo 2.2.2.25.1.3. del mencionado decreto:

> La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país. La transmisión de datos personales por su parte implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia y tiene por objeto la realización de un tratamiento por el Encargado por cuenta del Responsable[31].

De acuerdo con lo anterior, así como con el artículo 2.2.2.25.5.1. del decreto, la transferencia internacional de datos personales está prohibida a cualquier país que no cuente con un nivel adecuado de protección de estos. Tal prohibición no procede en distintos casos enumerados en el artículo 26 de la Ley 1581 dentro de los cuales están: (1) que cuente con la autorización expresa e inequívoca del titular, y (2) cuando se

[31] Véase http://www.sic.gov.co/preguntas7frecuentes7pdp.

trate de transferencias necesarias para la ejecución de un contrato entre el responsable y el encargado, caso en el cual no se necesitará de autorización del titular del dato. A raíz de esta última excepción, nace otra figura que también es relevante para el presente estudio: se trata del contrato de transmisión de datos personales, que se desarrolla en el artículo 2.2.2.25.5.2.

Principio de responsabilidad demostrada

A pesar de lo mencionado en relación con la normatividad colombiana en materia de protección de datos personales, esta no determina de manera específica qué medidas deben tomarse para garantizar la seguridad del tratamiento de las bases de datos en las cuales se procesa la información. Corresponde al responsable y encargado de la información implementar las medidas técnicas, administrativas y humanas que permitan asegurar tal fin. Sobre esto, el artículo 2.2.2.25.6.1 del decreto tratado indica que

> Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este capítulo, en una manera que sea proporcional a lo siguiente: 1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente. 2. La naturaleza de los datos personales objeto del tratamiento. 3. El tipo de Tratamiento. 4. Los riesgos potenciales que el referido tratamiento podría causar sobre los derechos de los titulares.

Así las cosas, los responsables y encargados de la información deben implementar medidas que permitan el cumplimiento de las exigencias legales en la materia y que este hecho sea demostrable ante las autoridades colombianas en el momento en que sea requerido.

Beneficios

La información es la gasolina del siglo XXI, y la analítica de datos el motor de combustión.

P. Sondergaard, 2017

A continuación, se ejemplificarán casos y sectores en los cuales el *big data* ha traído grandes beneficios.

Salud

El doctor Russ Altman, profesor de Medicina y Bioingeniería de Stanford, y su equipo hicieron un gran descubrimiento usando el *big data*. Así, lograron identificar que en las personas que tomaban por un largo periodo el medicamento llamado Paxil junto con otro conocido como Pravachol se observaban efectos colaterales, incluso mortales. Esta combinación ocasionaba que la glucosa de la sangre se elevara a niveles de diabetes. Si bien ambos medicamentos fueron aprobados para la venta al público y fueron debidamente examinados por la Food and Drug Administration (FDA) en Estados Unidos, fue imposible identificar de forma previa los efectos de combinarlos[32].

Este descubrimiento fue hecho gracias a que el equipo de investigadores utilizó técnicas de minería de datos y análisis estadístico para identificar estos patrones entre una gran cantidad de información. Para esto, se usó información recolectada de diferentes fuentes, incluyendo historias clínicas, bases de datos de más de treinta años de compañías farmacéuticas, entre otras. Por otro lado, los científicos con apoyo de Microsoft y usando el buscador Bing hicieron un proceso para identificar las búsquedas en esta herramienta que combinaran en una misma frase las palabras *Paxil* y *Pravachol* en conjunto con otras relacionadas con los síntomas de la diabetes[33].

[32] Sarah Bielecki, "Harnessing Big Data to Better Understand What Happens When We Mix Drugs" (2016), https://engineering.stanford.edu/magazine/article/harnessing-big-data-better-understand-what-happens-when-we-mix-drugs.

[33] *Ibid.*

Tráfico

Los gobiernos del mundo están estableciendo herramientas tecnológicas para la imposición de precios por movilidad basados en cantidad de movilización y nivel de congestión. De esta forma, los usuarios pagan dependiendo del uso de su vehículo y las vías por las que transiten. Igualmente, los planeadores urbanos se están beneficiando del análisis de la información sobre la ubicación personal para la toma de decisiones relacionadas con la construcción de vías, mitigación del tráfico y planeación para el desarrolla urbano. Al mismo tiempo que esto ocurre, los usuarios particulares se benefician de la posibilidad de planear de manera inteligente sus rutas, basadas en información en tiempo real sobre el tráfico, incluyendo reportes de accidentes e información sobre hora pico[20].

Retail

El *big data* también está transformando el mercado de *retail*. El sistema de administración de inventario de Wal-Mart llamado Retail Link fue uno de los pioneros en la era del *big data*, y permitía tener un registro del número de productos en cada estantería en tiempo real[34]. Otro ejemplo en el cual se puede ver el efecto *del big data* en el mercado de *retail* es el uso del algoritmo de Amazon "Clientes que compraron esto también compraron", que alienta a los consumidores a adquirir otros productos relacionados con su búsqueda por medio de diferentes filtros. De esta forma, las estrategias de negocio de este tipo de plataformas se están centralizando no en la identidad de cada cliente, sino en los atributos de su perfil como consumidor, lo que pasaría a determinar la naturaleza de la propaganda que recibe[35].

[34] "Real Vision Investment Case Study 2015", *The Economist*, 2010, 6. https://www.economist.com/sites/default/files/uaellermba_ws.pdf.

[35] Tene y Polonetsky, "Big Data for All", 2012.

Transacciones

Otra de las áreas en las que el *big data* otorga un gran valor es en la detección de fraudes financieros con las tarjetas bancarias. Teniendo en cuenta la gran cantidad de información que es capturada en el día a día por el comercio electrónico, se identificó la necesidad de crear mecanismos y soluciones para detectar movimientos sospechosos de las tarjetas bancarias. Para este fin, las entidades financieras desarrollaron sistemas que permiten predecir los fraudes financieros gracias a la detección de movimientos poco usuales o previamente identificados como sospechosos en tiempo real. Para poder lograr esto es necesario tener sistemas capaces de analizar el historial de transacciones de cada usuario y hacer una evaluación usando diferentes variables, como ubicación, monto y frecuencia, entre otros[36].

Si bien estos ejemplos muestran de forma general algunos de los usos benéficos de la tecnología del *big data,* también permiten identificar algunos indicios de los riesgos que trae consigo esta tecnología. Este será el tema del siguiente apartado.

Riesgos: *big data*, *big problem?*

Reproducción incremental: "Para Google sigo siendo deudor y casado"[37]

La acumulación de datos personales tiene un efecto adverso sobre la privacidad de los individuos. Una investigación puede dar conclusiones completamente distintas con pequeñas variaciones en las palabras de búsqueda[38]. Así, un experimento realizado en la Universidad de Texas

[36] Duncan Douglas, "An Examination of the Fraud Liability Shift in Consumer Card-Based Payment Systems", *Economic Perspectives*, n.º 33 (2009), https://www.chicagofed.org/publications/economic-perspectives/2009/1qtr2009-part7-douglass.

[37] "Mario Costeja: El español que golpeó al todopoderoso Google", *El Comercio*, 14 de mayo del 2014. https://elcomercio.pe/tecnologia/empresas/mario-costeja-espanol-golpeo-todopoderoso-google-319662-noticia/.

[38] Melissa Fach, "Stats on Facebook 2012 [Infographic]", *Search Engine Journal*, 17 de febrero del 2012, http://www.searchenginejournal.com/stats-on-facebook-2012-infographic/40301.

sobre la plataforma de Netflix demostró que usando una gran cantidad de información que había pasado por un proceso previo de desidentificación, con el objetivo de ofrecer las recomendaciones de películas en los perfiles de Netflix, y comparándola con una base de datos de publicidad disponible en la red lograron identificar la identidad real de los usuarios, rompiendo cualquier posibilidad de anonimato. Esto significa que la combinación de diferentes bases de datos unida a la capacidad masiva de procesamiento de información permite recrear el perfil real de una persona a partir de decisiones tan simples como los gustos en las películas[39].

La constante transmisión de información de una persona en el día a día muchas veces es incluso indetectable por ella misma, y esto hace que sea aún más difícil recapturarla o ejercer los derechos estudiados con anterioridad, como los de libertad, veracidad y circulación restringida.

Este cuestionamiento deriva en uno de los preceptos más importantes en materia de protección de datos personales y uno de los cuales se ve más en riesgo con el procesamiento masivo de la información: el derecho al olvido.

¿La información puede desaparecer?

Caso Costeja versus Google

En el 2009 Mario Costeja intentó sin éxito inicial que Google eliminara un enlace que redireccionaba a una publicación en 1998 en la que aparecía una propiedad embargada por deudas que se disponía a ser subastada. Un año después de esta solicitud, la Agencia de Protección de Datos española ordenó a Google suprimir esta información. Como respuesta a esta decisión, Google acudió ante el Tribunal de Justicia de la Unión Europea, quien reiteró la decisión de la agencia española y sostuvo que debía buscarse un equilibrio entre el derecho individual a la privacidad

[39] Arvind Narayanan y Vitali Shmatikov. "Robust De-Anonymization of Large Sparse Datasets" (ponencia presentada en el IEEE Symposium on Security & Privacy, 2008).

y la protección de los datos, reconociendo así el derecho a que se elimine de internet la información personal[40].

El concepto de derecho al olvido en Colombia se analizó por primera vez en Colombia a partir de la Sentencia T-414 de 1992[41]. Al inicio, este derecho se centraba en situaciones de reporte de personas morosas o que hubiesen cometido un delito, pero dado el desarrollo tecnológico actual y la multiplicidad de plataformas en las cuales se comparten datos de distintas naturalezas, este derecho ha empezado a ser relevante en otras esferas de la vida privada de las personas.

La efectividad para garantizar el derecho al olvido depende en gran medida del contexto en el que se pretenda aplicar, ya que no es lo mismo tratar de ejercer frente a una central de información de riesgo crediticio local que ante cualquier persona o empresa que publica información en internet. Esto atiende a que

> […] es muy difícil conseguir la "desaparición" definitiva de la información en internet, entre otros, porque la misma puede ser publicada o replicada en la red por millones de personas, o por la complejidad y el desconocimiento del cambiante e innovador mundo tecnológico, el cual no alcanza a ser entendido por muchos de nosotros, por algunos jueces, funcionarios públicos o reguladores[42].

La misma Corte Constitucional en Colombia ha admitido que

> […] la información que se comparte en internet deja una huella que, […] hace posible rastrear e identificar todo lo que una persona hizo en el mundo virtual, los lugares que visitó o consultó y los productos que consumió a través de la red. La recopilación de estos datos puede ser utilizada para crear perfiles sobre los gustos, preferencias, hábitos de consulta y consumo de las personas que emplean internet (como simples

[40] "Mario Costeja", 2014.

[41] C. Const., Sent. T-414/1992. M.P. Ciro Angarita Barón.

[42] Nelson Remolina, "¿Derecho al olvido en el ciberespacio?: Principios internacionales y reflexiones sobre las regulaciones latinoamericanas". En *Hacia una internet libre de censura II*, compilado por Agustina del Campo (Ciudad Autónoma de Buenos Aires: Universidad de Palermo, 2017).

usuarios o como agentes económicos que desarrollan sus actividades por este medio)[43].

Análisis predictivo

> *Es más fácil ocultar una infidelidad a tu pareja que a Google, que no tarda en ponernos anuncios de escapadas de fin de semana cuando nos lee mensajes románticos.*
>
> A. Suárez, *Desnudando a Google*

El *big data* permite realizar un análisis predictivo que puede ser útil para anticiparse a enfermedades, crímenes u otro tipo de conductas. En una historia publicada en el 2012, el *New York Times* expuso un caso de la compañía de *retail* Target, que desarrolló un sistema de puntaje que es capaz de predecir un embarazo basándose en los hábitos de compra de los clientes[44]. El caso que desató polémica consistía en que un padre de una adolescente se presentó molesto ante Target porque su hija estaba recibiendo cupones y propaganda relacionados con productos para bebés. Unos días después, este mismo hombre llamó a la tienda y se disculpó admitiendo que, de hecho, su hija estaba embarazada.

En la aplicación Rappi[45] existe un sistema que detecta las entradas que se hacen a ella y va recolectando información que permite identificar a qué horas normalmente se consume y cuáles son los productos que por lo general se ordenan. El mismo hecho de que haya un ingreso a la aplicación y no resulte en una orden puede hacer que se genere un mensaje al consumidor recordándole que el producto sigue disponible.

La Corte Constitucional define el derecho a la intimidad como

[43] C. Const., Sent. C-1147/2001. M.P. Manuel José Cepeda Espinosa.

[44] Charles Duhigg, "How Companies Learn Your Secrets", *The New York Times Magazine*, 16 de febrero del 2012.

[45] Rappi es una aplicación por medio de la cual se pueden solicitar productos y servicios a domicilio.

> […] la esfera de protección del ámbito privado del individuo y de su familia, la cual se traduce en una abstención de conocimiento e injerencia en aquella órbita reservada que le corresponde a la persona y que escapa al conocimiento público y, por tanto, no debe ser materia de información suministrada a terceros ni de intervención o análisis de grupos ajenos, ni de divulgaciones o publicaciones[46].

Bajo este supuesto sería difícil alegar que en un caso como el publicado por el *New York Times*, en el que Target supo antes que el padre de la adolescente del embarazo de esta, no es una forma de vulnerar esa esfera privada de las personas.

La Corte Constitucional en diferentes ocasiones ha reiterado que el ser humano goza de la garantía de determinar qué datos quiere que sean conocidos y tiene derecho a determinar lo que se denomina "imagen informática"[47]. Esto trae consigo un reto para el principio de finalidad, por cuanto no es claro para los titulares de los datos hasta qué punto va a llegar el análisis practicado a estos. Cuando un supermercado recolecta los datos de sus clientes normalmente pide información como el nombre, el número de identificación, el celular, lugar de residencia, entre otros. Una vez el cliente queda inscrito en esa base de datos no es perceptible que en adelante cualquier producto o compra que se realice va a quedar sujeta a un perfil específico y va a ser capaz de predecir en algún momento las necesidades, los gustos, las enfermedades y otros tipos de características que pueden llegar incluso a ser asociados con datos sensibles[48].

Por otro lado, también se ve vulnerado el principio de libertad, en la medida en que la calidad de la autorización que un titular está otorgando a un supermercado al dar su nombre difícilmente deja ver de una manera consciente, previa, expresa e informada el tratamiento que en realidad se está efectuando sobre los datos recolectados y los efectos de su autorización.

[46] C. Const., Sent. C-872/2003. M.P. Clara Inés Vargas.

[47] C. Const., Sent. C-748/2011. M.P. Jorge Ignacio Pretelt.

[48] Se entiende como datos sensibles "[…] aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas […]", entre otros. L. 1581/2012, art. 15.

Finalmente, también afecta el principio a la veracidad de la información, puesto que la falta de conciencia de los perfiles que las compañías desarrollan sobre los consumidores hacen casi imposible que los titulares exijan su rectificación.

Cruce de bases de datos: ¿limitarlo es la respuesta?

Tanto el Departamento Administrativo de Catastro Distrital Capital como la Superintendencia Nacional de Salud dispusieron una página web que incorporaba bases de datos, la primera sobre la información catastral con la cual se podía relacionar a un sujeto con información como su dirección, tipo de propiedad, estrato, área de terreno, entre otros, y la segunda sobre información relativa a la afiliación al régimen de seguridad social, personas beneficiarias, fecha de afiliación, mora…

En virtud de lo anterior, el ciudadano Carlos Antonio Ruiz interpuso acción de tutela contra las dos entidades por considerar que la disponibilidad de esta información en línea violentaba su derecho a la intimidad, entre otros[49]. En la citada providencia, la Corte Constitucional indicó que estas conductas desconocían los principios de libertad, finalidad y circulación restringida, por cuanto las entidades debían abstenerse de "realizar conductas que faciliten el cruce de datos y la construcción de perfiles individuales" ya que "al facilitar las condiciones para que la misma sea sumada a otra, con el concurso de diversas fuentes de información, vulnera su derecho a la autodeterminación informática".

Teniendo en cuenta este análisis de la Corte Constitucional, ¿sería posible hacer *big data* en Colombia cuando esta corporación está limitando la posibilidad de cruzar bases de datos? Ya se han visto los grandes beneficios que trae consigo la inteligencia de datos, que además es solo la base para el desarrollo de muchas otras tecnologías como la inteligencia artificial, el internet de las cosas, entre otros. ¿La solución debe ser limitar la posibilidad de usar este tipo de técnicas de analítica de datos? Una revisión más detallada de estas preguntas se hará más adelante.

[49] C. Const., Sent. T-729/2002. M.P. Eduardo Montealegre Lynett.

Actos discriminatorios y excluyentes: el borde ético

En mayo del 2014 la Casa Blanca expidió un reporte titulado *Big Data: Seizing Opportunities, Preserving Values* (Podesta Report) en el cual se evidenciaba el potencial de discriminación que traía consigo esta técnica. De acuerdo con el reporte, esta forma de analítica de datos tiene la capacidad de eclipsar la normatividad desarrollada alrededor de la protección del tratamiento de datos, especialmente en campos como el acceso a la vivienda, el empleo, las solicitudes de crédito, salud y educación.

Por definición, el *big data*, al realizar minería de datos, siempre va a estar ligado a alguna forma de discriminación estadística[50]. Cuando se habla de este tipo de discriminación se hace referencia a un proceso por medio del cual se automatiza la identificación de una serie de patrones y singularidades sobre las cuales se pueda tomar una decisión. El conjunto de estos patrones y singularidades relacionadas entre sí es lo que se conoce como *modelo*, y puede ser usado para automatizar el proceso de clasificación de entidades, perfiles o actividades, estimando variables que no habían sido identificadas previamente y prediciendo resultados[51].

El *big data* puede reforzar patrones existentes de discriminación por medio de los sistemas de tomas de decisiones automatizadas, o crear nuevos espacios en los que se reproduzca la discriminación.

Toma de decisiones automatizadas

En su libro *The Daily You: How the New Advertising Industry Is Defining your Identity and your Worth* Joseph Turow argumenta que el aumento en la personalización de información que recibe un individuo, basada en algoritmos que identifican un perfil específico, representa

[50] Andrew Selbst Solon Barocasy, "Big Data's Disparate Impact". *California Law Review*, n.º 104 (2016): 671.

[51] Michael Berry y Gordon Linoff. "*Data Mining Techniques: For Marketing, Sales, and Customer Relationship Management*" (Indianapolis, Indiana: Wiley Publishing, 2004), 37.

un riesgo para el discurso social y democrático[52]. Turow explica que al asignar un individuo a una categoría previamente establecida, la toma de decisiones automatizadas segmenta a la sociedad en pequeños grupos que definen la información, los productos y las oportunidades a las cuales tienen acceso.

Frente a este tipo de segmentación surge una inquietud a la luz de la normatividad colombiana relacionada con el derecho al libre desarrollo de la personalidad, consagrado en el artículo 16 de la Constitución Política de Colombia. La Corte Constitucional ha indicado que este "configura la defensa de la condición ética de la persona que la hace instancia suprema e irreductible de sus propias decisiones, pues solo le incumben a ella y además, determinan su propio destino como sujeto de derechos autónomo, responsable y diferenciado"[53]. Se define entonces como la protección de que las personas gozan para autodeterminarse, lo que implica desarrollar sus planes de vida sin ningún tipo de injerencia mientras que no se vea afectado el orden jurídico ni los derechos de un tercero[54].

En este sentido, la toma de decisiones automatizadas que segmentan a la sociedad dentro de grupos preestablecidos evidentemente contraría los supuestos del derecho al libre desarrollo de la personalidad, por cuanto obstruye el libre desarrollo de una persona a autodeterminarse limitando o exponiendo de forma completamente intencionada el acceso a las diferentes opciones en el mercado.

Se presentan casos como el de Facebook, que escandalizó a la sociedad hace un tiempo, según el cual esta compañía supuestamente admitió poder identificar a adolescentes que se sientan "poco valorados", "inseguros" y con "necesidad de una dosis de confianza" para buscar venderles productos que les ayuden a satisfacer estas necesidades[55].

Algunos Estados han intentado regular la toma de decisiones automatizada. Una de las regulaciones más conservadoras relacionada con

[52] Joseph Turow, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth* (Yale University Press, 2011).

[53] C. Const., Sent. T-030/2017. M.P. Gloria Stella Ortiz.

[54] C. Const., Sent. T-909/2011. M.P. Juan Carlos Henao Pérez, entre otras.

[55] "Facebook Told Advertisers It Can Identify Teens Feeling 'Insecure' and 'Worthless'", *The Guardian* (2017), https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens.

temas de *big data* es la de la Unión Europea. Un ejemplo de cómo se aborda el riesgo que trae consigo la toma de decisiones automatizadas es lo dispuesto por el considerando 71 del Reglamento (UE) 2016/679 (RGPD), en cuyo texto se lee:

> El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar, como la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna. Este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Espacios en los que se reproduce la discriminación

En Colombia, ha habido casos en los que se demuestra que la discriminación no se da únicamente como resultado de un proceso de análisis de datos, sino por la exclusión de estos. Así, en la sentencia de Tutela 167 del 2016 la Corte Constitucional falló un caso en el cual se alegaba una vulneración al derecho fundamental a la vivienda en Colombia[56] cuando la información de un ciudadano no fue incluida en distintas bases de datos administradas por el Ministerio de Vivienda, Fonvivienda y el Departamento para la Prosperidad Social lo que le impedía acceder a los beneficios de un subsidio de vivienda familiar. Esto ocurre ya que las entidades del Gobierno nacional cuentan con bases de datos

[56] C. N., art. 51: "todos los colombianos tienen derecho a vivienda digna. El Estado fijará las condiciones necesarias para hacer efectivo este derecho y promoverá planes de vivienda de interés social, sistemas adecuados de financiación a largo plazo y formas asociativas de ejecución de estos programas de vivienda".

mediante las cuales se incorpora información para la asignación de beneficios relacionados, por ejemplo, con la educación, la salud, atención de víctimas y vivienda.

La Corte falló el caso a favor del accionante, alegando que en desarrollo anterior había establecido como un principio al que debía sujetarse la administración de los datos el de "incorporación", que se ejerce

> […] cuando de la inclusión de datos personales en determinadas bases, deriven situaciones ventajosas para el titular, la entidad administradora de datos estará en la obligación de incorporarlos, si el titular reúne los requisitos que el orden jurídico exija para tales efectos, de tal forma que queda prohibido negar la incorporación injustificada a la base de datos[57].

Así, la Corte Constitucional en Colombia ha reconocido que "el derecho al *habeas data* no solo es una herramienta para solucionar una aparente tensión entre la intimidad y el interés general sino que además, en determinadas circunstancias, es el medio que permite el ejercicio efectivo de otros derechos fundamentales"[58] los cuales pueden ser vulnerados cuando se omite el tratamiento de los datos o este es arbitrario.

La jurisdicción: un problema transversal

Caso Canadá vs. Google

La Suprema Corte de Justicia de Canadá dictó una sentencia que obligaba a Google a eliminar por completo en su buscador cualquier referencia a nivel mundial que estuviese relacionada con una empresa identificada como Datalink Technologies Getaways, que usaba varios sitios web para comercializar a nombre propio productos y servicios que son de propiedad exclusiva de una empresa canadiense llamada Equustek.

Tras esta orden judicial, Google cumplió lo solicitado únicamente para el territorio canadiense, lo que hacía que una búsqueda hecha por

[57] C. Const., Sent. T-729/2002. M.P. Eduardo Montealegre Lynett.

[58] C. Const., Sent. T-167/2016. M.P. Alejandro Linares Cantillo.

un servidor ubicado por fuera de esta jurisdicción aún pudiese arrojar resultados asociados con Datalink Technologies Getaways. La Corte de Justicia ha expedido más aclaraciones de los efectos de la sentencia, en las cuales se solicita aplicar esta medida a nivel mundial, a lo cual Google se ha negado[59].

En Colombia, la misma Corte Constitucional ha identificado que internet es una plataforma "cuyos efectos a nivel transnacional plantea diversos problemas constitucionalmente relevantes"[60]. Dentro de la citada providencia, se pone en evidencia que no es una realidad jurídica inocua el desarrollo exponencial de una red mundial de comunicaciones por medio de la cual la información se convierte en una materia de fácil acceso y circulación. Frente a esto, indica que "En este nuevo escenario tecnológico, en pleno desarrollo, los mandatos expresados en la Carta Política cobran un significado sustancial que demanda del juez constitucional la protección de los derechos reconocidos a todas las personas, pues se trata de garantías que también resultan aplicables en ese ámbito". Esto significa que a los ojos de la Corte Constitucional en Colombia, así se cree una realidad virtual no necesariamente adjudicada a un territorio específico, el juez constitucional también está llamado a velar por el goce efectivo de los derechos en el ciberespacio.

A pesar de lo anterior, esta misma corporación reconoce, en la sentencia referida, que

> […] debido a la rapidez con la que evoluciona la tecnología que se emplea en internet, y al ingenio y creatividad de muchos de sus operadores, los preceptos jurídicos expedidos con el propósito de regular las actividades que se desarrollan por este medio de comunicación pueden resultar inocuos para alcanzar algunas de las finalidades que persiguen.

De esta forma, frente al terreno de la jurisdicción y la capacidad de vincular judicialmente a compañías multinacionales que prestan servicios desde territorios extranjeros, sigue habiendo un gran reto para la regulación, no solo colombiana, sino también global. Casos como estos,

[59] "Google Must Delete Search Results Worldwide, Supreme Court of Canada Rules", *Fortune* (2017). http://fortune.com/2017/06/28/canada-supreme-court-google.

[60] C. Const., Sent. C-1147/2011. M.P. Manuel José Cepeda Espinosa.

por ejemplo, se han presentado también en Colombia. La Sentencia T-040 del 2013 hace alusión a un caso en el cual un ciudadano interpuso una tutela en contra de casa Editorial El Tiempo S. A. y de Google Colombia Ltda. con el objetivo de que eliminaran una noticia que hacía referencia a un proceso en el cual el accionante estuvo involucrado[61].

Frente a este caso y la posibilidad de eliminar este resultado de búsqueda, la Corte Constitucional indicó que cuando se habla de un *motor de búsqueda* se hace referencia al "fichero de una gran biblioteca que es internet y como tal, por su intermedio se ordenan las páginas de internet que, siguiendo con el ejemplo dado, serían los libros de esa supuesta biblioteca". Esto significa que la información que es ingresada a internet por los dueños de las páginas es la que determina cuál es el resultado que los usuarios de los motores de búsqueda van a recibir.

En este sentido, esta providencia también es clara al indicar que "el responsable de la información emitida, y por ende de su posible rectificación, es el medio de comunicación que recolectó, analizó, procesó y divulgó la noticia", lo cual en este caso hace alusión a la página indicada en el documento de reclamación, pero que en ningún caso sería el motor de búsqueda, ya que este ni redacta ni publica tal información, y por ende no se le puede endilgar la responsabilidad sobre la veracidad o imparcialidad de un respectivo artículo, noticia o columna que aparezca en sus resultados.

Por otro lado, en la Sentencia con número de expediente T-5.771.452 del 2017[62] se ve otro desarrollo de la Corte Constitucional frente a un tema similar. En el 2014 una persona de forma anónima publicó mediante la herramienta Blogger.com, propiedad de Google Inc., un comunicado difamatorio relacionado con el negocio del accionante. Este le solicitó a Google varias veces que eliminara este blog, solicitud a la que Google se negó en todas las oportunidades. Frente a este caso, la Corte Constitucional ordenó a Google eliminar el mencionado comunicado por cuanto su contenido imputaba de forma anónima información no probada sobre la comisión del delito de estafa. A grandes rasgos, la conclusión de la Corte fue que Google estaba vulnerando los derechos fundamentales a la intimidad, honra y buen nombre, puesto que las publicaciones falsas y difamatorias, a pesar de hacerse en una herramienta

[61] C. Const., Sent. T-040/2013. M.P. Jorge Ignacio Pretelt.

[62] C. Const., Sent. T-5.771. 452/2017. M.P. Jorge Iván Palacio Palacio.

que solo se encarga de procesar, son de carácter anónimo por lo que la reclamación en caso de afectaciones o solicitudes de eliminación de contenido dejan sin recursos efectivos a los afectados cuando no pueden comunicarse con los creadores de los blogs o tener información de ellos; por ende, debe ser el propietario de la plataforma quien permita la efectiva protección de estos derechos.

Lo anterior demuestra, justamente, los grandes retos que implica para el regulador el conflicto de jurisdicción que se da a través del uso de herramientas como el *big data*. Aquí se ve reflejada la intención de proteger los derechos de los titulares de los datos de acuerdo con los principios de cada regulación, frente a la impotencia que implica no poder trascender los efectos de una decisión judicial en un espacio que no tiene fronteras.

Prácticas para la sana explotación de los datos

Algunas herramientas bajo la legislación colombiana

De conformidad con los artículos 14 y 15 de la Ley 1581 del 2012 los titulares de la información cuentan con la posibilidad de consultar cualquier información personal que repose en base de datos pública o privada. Esta deberá ser suministrada al titular por parte del responsable o el encargado, bien porque se tenga un registro individual o porque sea posible asociarla a su identidad.

A fin de facilitar este proceso, tanto el responsable como el encargado deberán tener algún medio para realizar esta consulta, la cual deberá ser respondida en un término no mayor a diez días hábiles. De forma específica, el artículo 15 de la citada ley regula las reclamaciones que puede hacer el titular con el objetivo de corregir, actualizar o suprimir la información contenida en la base de datos o elevar el reclamo cuando se identifique un incumplimiento de los deberes establecidos en la mencionada normativa.

Asimismo, a la luz del artículo 13 de la Ley 1266 del 2008 se desarrolla en Colombia la permanencia del dato negativo. Esta norma, en concordancia con la Sentencia C-1011 del 2008[63], por medio de la cual

[63] C. Const., Sent. C- 1011/2008. M.P. Jaime Córdoba Triviño.

se relacionan los planteamientos jurisprudenciales de la caducidad de la información de contenido financiero y crediticio de manera negativa, le ha permitido a la SIC compartir en distintas ocasiones la regla jurídica aplicable a este caso:

> Es claro que la información de datos personales de carácter negativo debe estar supedita [sic] a que sean útiles y pertinentes para el cálculo del riesgo financiero, y por ello, no se concibe que duren indefinidamente en el tiempo cuando pierden su funcionalidad. Por lo anterior, la aplicación analógica de la prescripción de la acción ordinaria (el mecanismo procesal que le permite a un acreedor obtener una declaración judicial respecto de la existencia de una obligación), conlleva a [sic] que se tome el término de 10 años contados a partir de su exigibilidad, en los casos en que el titular de la información no haya procedido al pago de su obligación. Por su parte, el término de permanencia del dato negativo de la información consagrado en el artículo 13 de la Ley 1266 de 2008, es de 4 años a partir de la extinción de la obligación por cualquier modo[64].

Así, se observan algunos ejemplos de desarrollo tanto legal como normativo de las herramientas que tienen los titulares de los datos en Colombia para hacer valer sus derechos constitucionales.

Minimización de los datos

Después de varias iteraciones y formulaciones, la minimización de los datos que se generan sigue siendo un pilar fundamental de las normativas relacionadas con la regulación de su tratamiento (OECD Guidelines). Se sigue pidiendo a las organizaciones que mantengan limitada la recolección de datos personales a lo mínimo necesario para obtener sus objetivos legítimos. Como se ha visto en este texto, también se les ha pedido que eliminen los datos que ya no sean necesarios para cumplir con sus propósitos, para reforzar así las políticas de retención de la información.

[64] Concepto Superintendencia de Industria y Comercio. Radicación: 17-93019-2 del 2017.

Si bien esta es una medida que no se puede pasar por alto, tampoco puede ser la base para garantizar el cumplimiento de los principios rectores del tratamiento de los datos ni en Colombia ni en el mundo, por lo que se hace relevante seguir explorando otro tipo de medidas.

Control individual

Los marcos normativos alrededor del mundo continúan haciendo énfasis en el consentimiento o en el control individual como un principio fundamental en el régimen de protección de datos. Un ejemplo de esto es la legislación colombiana, cuya piedra angular para el tratamiento de datos continúa siendo la autorización previa, expresa e informada.

Una de las problemáticas que esto provoca es que en ocasiones se pueden incluso llegar a exigir obligaciones irreales. Por un lado, las organizaciones se ven en la necesidad de dar a conocer sus políticas de tratamiento en ventanas en internet poco llamativas, que en general se enfrentan con consumidores que tienen poco interés en entender lo que dice la "letra pequeña". Por otro lado, se espera de estos individuos que lean, entiendan declaraciones complicadas de responsabilidad y expresen su consentimiento informado. Estudios han demostrado que para poder leer todas las políticas de privacidad de los productos que se consumen en un día habitual, un individuo común necesitaría aproximadamente treinta días al año[65].

Anonimización y seudonimización

Como ya se había dicho, la definición de dato personal, según la Ley 1581 del 2012, es: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. En este sentido, es pertinente analizar cuándo una información puede asociarse a una persona, y si la separación entre la información y

[65] Aleecia McDonald y Lorrie Faith, "The Cost of Reading Privacy Policies", *A Journal of Law and Policy for the Information Society* 4, n.º 3 (2008).

su adjudicación a una persona determinada puede ser una herramienta que ayude a garantizar los derechos ya desarrollados en el presente documento.

El RGPD establece al respecto que

> […] los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo.

Así pues, los datos deben procesarse de tal forma que ya no se puedan usar para identificar a la persona mediante la aplicación de "todos los medios" dispuestos de forma razonable por el responsable de la información o por un tercero, debiendo garantizar, asimismo, que el proceso de desidentificación del dato llegue a un nivel en el que el mismo sea irreversible (Grupo de Trabajo sobre Protección de Datos del Artículo 29, UE 2014[66]).

En términos generales, existen dos enfoques diferentes de la anonimización, el primero se basa en la aleatorización, y el segundo, en la generalización. La primera busca modificar la veracidad de los datos con el objetivo de eliminar el vínculo que existe entre estos y la persona usando técnicas para crear ambigüedad, como por ejemplo la "adición de ruido", que consiste en modificar los atributos de los datos para disminuirles exactitud. Por otro lado, la generalización tiene el objetivo de diluir los atributos de los datos modificando así las escalas u órdenes de magnitud.

Por otro lado, existe otro tipo de proceso llamado seudonimización. El RGPD lo define como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable". Así, la seudonimización reduce la capacidad de cruce de datos de forma tal que no permite identificar a un individuo en concreto,

66 Comité Europeo de Protección de Datos (antes Grupo de Trabajo del Artículo 29).

pero si se aplica de forma exclusiva es probable que tras un proceso de seudonimización pueda re-identificarse al titular de la información si se vuelven a incluir los datos modificados o excluidos[67] (Grupo de Trabajo sobre Protección de Datos del Artículo 29, UE 2014).

Este tipo de técnicas para separar la identidad física de los datos que son generados en el día a día puede ser una de las opciones más prósperas para garantizar la protección de los datos personales y, a su vez, usarlos como materia prima para continuar desarrollando todos los beneficios del tratamiento de la información.

Algunos retos en Colombia: cómo prepararnos para la nueva era

En este momento, el Departamento Nacional de Planeación está elaborando el documento CONPES para el desarrollo de la política de explotación de datos en Colombia. Uno de los aspectos más destacables de este es el análisis que se hace de las condiciones actuales del país y cómo estas contribuyen o afectan la posibilidad de alcanzar resultados materiales mediante las políticas de explotación.

La baja digitalización en Colombia es un gran reto para las entidades públicas, pues un porcentaje bastante considerable continúa haciendo el registro digital desde el papel. Es claro, después del análisis realizado en este texto, que no se puede hacer ningún tipo de proceso de analítica de datos si no hay datos que analizar, o están en un formato difícil de procesar. Por esta razón, el primer paso para poder garantizar un desarrollo óptimo es empezar a desarrollar dentro de las entidades una cultura de la digitalización.

Ahora bien, otro gran reto que tienen las entidades públicas es que, una vez se haya hecho un proceso apropiado de digitalización de información, estas sean capaces de compartirla entre sí para lograr encontrar relaciones distintas[68]. El nivel de interoperabilidad que tienen las entidades públicas en Colombia es bastante bajo. Si no se dan estas condiciones, es difícil garantizar la optimización de los recursos de información,

[67] *Ibid.*

[68] DNP. *Documento CONPES 3920. Política de explotación de datos* (2017).

que, como cualquier otro, deben ser usados de forma que permita obtener el mayor beneficio. Este tipo de actividades podría llegar a ser impulsado mediante estandarizaciones para el registro administrativo de la información y otro tipo de mecanismos que simplifiquen su almacenamiento.

Reflexiones finales

La era del *big data* ya llegó y está en muchos aspectos de nuestro día a día. Desde ejemplos como los casos de David contra Goliat en la Unión Europea, hasta el mensaje que llega al celular con frecuencia y es pasado por alto, el objetivo principal de este texto era alertar al lector de que el *big data* no es ajeno a ninguna persona y que por "*big*" que sea, es capaz de identificar y de sustraer la información a un nivel de detalle del cual pocos son conscientes.

Los beneficios que trae consigo la explotación de datos aún no han sido dimensionados y cada vez más se van desafiando fronteras de lo que se creía posible. Si bien es importante fomentar el uso de este tipo de herramientas, debe haber claridad del marco normativo y los límites dentro de los cuales debe expandirse. En Colombia se ha visto un desarrollo constante de los principios que regulan este ejercicio. La Corte Constitucional ha sido pionera y ha marcado la pauta para la protección de los datos personales en el país. Se debe continuar con este desarrollo teniendo en cuenta dos factores importantes: (1) la estimulación de una cultura de protección de datos en el país que les permita a los ciudadanos tener presente qué recursos tienen, tanto normativos como propios, para proteger su propia información; y (2) la gran área de oportunidad que hay en Colombia, especialmente al nivel de las entidades públicas, para adoptar políticas que permitan optimizar toda la información que almacenan y que sea posible tratar. Esto, sin duda, traería un beneficio significativo a la forma en la que se diseñan las políticas públicas y se identifican las problemáticas reales de los ciudadanos. Logramos ver que el país cuenta con una variedad de herramientas para asegurar la protección de sus datos, por ejemplo la regulación en torno a la transferencia y transmisión de datos personales y el principio de responsabilidad demostrada; asimismo, cuenta con una entidad como la SIC, que está permanentemente desarrollando modelos y prácticas para la adopción segura de estas tecnologías. Pero no solo está en manos del regulador, sino de

nosotros mismos generar prácticas de las cuales se deriven efectos materiales de los principios para la protección de datos personales. Esta es una invitación para enterarse y ser conscientes de ahora en delante de la relevancia de este tema para todas las personas y del poder que tiene cada uno para decidir cómo son tratados sus datos.

Bibliografía

Anderson, Chris. "The end of theory: The data deluge makes the scientific method obsolete". *Wired.* 3 de junio del 2017. https://www.wired.com/2008/06/pb-theory/.

Aurik, Johan "La Cuarta Revolución Industrial tendrá un efecto disruptivo sobre el empleo, ¿pero, cómo?". *The World Economic Forum*, 30 de enero del 2017. https://www.weforum.org/es/agenda/2017/01/la-cuarta revolucion-industrial.

Barocas, S. y A. Selbst. "Big Data's Disparate Impact". *California Law Review* (2016).

Berry, Michael y Gordon Linoff. *Data Mining techniques: For marketing, sales, and customer relationship management*. Indianapolis, Indiana: Wiley Publishing, 2004.

Bielecki, Sarah. "Harnessing big data to better understand what happens when we mix drugs". 2016. https://engineering.stanford.edu/magazine/article/harnessing-big-data-better-understand-what-happens-when-we-mix-drugs.

Bignami, Francesca. "European versus American Liberty: A comparative privacy analysis of antiterrorism data mining". *Boston College Law Review* 48, n.º 3 (2007): 609-698.

Brynjolfsson, Erik. "Strength in numbers: How does data-driven decision-making affect firm performance?". *SSRN Electronic Journal*, n.º 1 (2011). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819486.

Comité Europeo de Protección de Datos (antes Grupo de Trabajo del Artículo 29). Comisión Europea. https://ec.europa.eu/newsroom/article29/items.

Desjardins, Jeff. "How much data is generated each day?". *The World Economic Forum*, 17 de abril del 2019. https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/.

Douglas, Duncan. "An examination of the fraud liability shift in consumer card-based payments". *Economic Perspectives*, n.º 33 (2009). https://www.

chicagofed.org/publications/economic-perspectives/2009/1qtr2009-part7-douglass.

Duhigg, Charles. "How companies learn your secrets". *The New York Times Magazine*, 16 de febrero del 2012.

"Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'". *The Guardian*, 2017. https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens.

Fach, Melissa. "Stats on Facebook 2012 [Infographic]". *Search Engine Journal*, 17 de febrero del 2012. http://www.searchenginejournal.com/stats-on-facebook-2012-infographic/40301.

"Google must delete search results worldwide, Supreme Court of Canada rules". *Fortune* (2017). http://fortune.com/2017/06/28/canada-supreme-court-google.

Hastia, Trevor, Robert Tibshirani y Jerome Friedman. *The elements of statistical learning: Data mining, inference, and prediction*. Nueva York: Springer, 2009.

http://www.google.com/intl/en/about/products/index.html.

"Manejo de información personal, '*habeas data*'". sic.gov.co/manejo-de-informacion-personal.

Manyika, James, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson y Alex Marrs. "Disruptive technologies: Advances that will transform life, business, and the global economy". *Mckinsey*, 1.º de mayo del 2013. https://www.mckinsey.com/businessfunctions/digital-mckinsey/our-insights/disruptive-technologies.

"Mario Costeja: El español que golpeó al todopoderoso Google". *El Comercio*, 14 de mayo del 2014. https://elcomercio.pe/tecnologia/empresas/mario-costeja-espanol-golpeo-todopoderoso-google-319662-noticia/.

McDonald, Aleecia y Lorrie Faith. "The cost of reading privacy policies". *A Journal of Law and Policy for the Information Society* 4, n.º 3 (2008).

Narayanan, Arvind y Vitali Shmatikov. "Robust de-anonymization of large sparse datasets". Ponencia presentada en el IEEE Symposium on Security & Privacy, 2008.

National Institute of Standards and Technology (NIST), United States Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-145/final.

Perlrot, Nicole. "Revamping at Yahoo to focus on its media properties and customer data". *The New York Times*, 11 de abril del 2012. http://bit.ly/HUneMM.

"Real vision investment case study 2015". *The Economist*, 2010. https://www.economist.com/sites/default/files/uaellermba_ws.pdf.

Remolina, Nelson. "¿Derecho al olvido en el ciberespacio?: Principios internacionales y reflexiones sobre las regulaciones latinoamericanas". En *Hacia una internet libre de censura II*, compilado por Agustina del Campo, 199-226. Ciudad Autónoma de Buenos Aires: Universidad de Palermo, 2017.

Rubinstein, Ira. "Big data: The end of privacy or a new beginning?". *International Data Privacy Law* 3, n.º 2 (mayo del 2013): 74-87.

Schwab, Klaus. "The fourth Industrial Revolution". *The World Economic Forum,* 14 de enero del 2016. https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab.

Sondergaard, Peter. Gartner Symposium/ITxpo. Octubre del 2011, Orlando, Florida.

Tene, Omer y Jules Polonetsky. "Big data for all: Privacy and user control in the age of analytics". *Northwestern Journal of Technology and Intellectual Propert*y (2012).

Turow, Joseph. *The daily you: How the new advertising industry is defining your identity and your worth*. New Haven: Yale University Press, 2011.

Jurisprudencia

C. Const., Sent. C-1011/2008. M.P. Jaime Córdoba Triviño.

C. Const., Sent. C-1147/2001. M.P. Manuel José Cepeda Espinosa.

C. Const., Sent. C-748/2011. M.P. Jorge Ignacio Pretelt.

C. Const., Sent. C-872/2003. M.P. Clara Inés Vargas.

C. Const., Sent. C-913/2010. M.P. Nilson Pinilla Pinilla.

C. Const., Sent. SU-082/1995. M.P. Jorge Arango Mejía.

C. Const., Sent. T-030/2017. M.P. Gloria Stella Ortiz.

C. Const., Sent. T-040/2013. M.P. Jorge Ignacio Pretelt.

C. Const., Sent. T-161/1993. M.P. Antonio Barrera Carbonell.

C. Const., Sent. T-176/1995. M.P. Eduardo Cifuentes Muñoz.

C. Const., Sent. T-340/1993. M.P. Carlos Gaviria Díaz.

C. Const., Sent. T-361/2014. M.P. Jorge Ignacio Pretelt.

C. Const., Sent. T-414/1992. M.P. Ciro Angarita Barón.

C. Const., Sent. T-729/2002. M.P. Eduardo Montealegre Lynett.

C. Const., Sent. T-909/2011. M.P. Juan Carlos Henao Pérez.

C. Const., Sent. T-5.771. 452/2017. M.P. Jorge Iván Palacio Palacio.

Constitución Política de Colombia. *Gaceta Constitucional* n.º 116. 20 de julio de 1991.

Decreto Único Reglamentario 1074 del 26 de mayo del 2015.

Ley Estatutaria 1581 del 2012, 18 de octubre del 2012, por la cual se dictan disposiciones generales para la protección de datos personales. *Diario Oficial* 48587.

Ley Estatutaria 1266 del 2008, 31 de diciembre del 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. *Diario Oficial* 47219.

Capítulo III

Inteligencia artificial en el mercado: presagios sobre la aplicación del régimen de competencia desleal[*, **]

José Fernando Sandoval Gutiérrez

Introducción

En este artículo se plantea la problemática que, en no muchos años, podría desencadenar la utilización de inteligencia artificial (IA) en el ejercicio de concurrencia al mercado, de cara a la aplicación del actual régimen de competencia desleal con el que contamos en Colombia. Esta problemática se analiza desde tres estadios distintos que siempre se deben agotar para poder analizar un comportamiento a la luz de la Ley 256 de 1996 o ley de competencia desleal, así como para establecer la deslealtad de la conducta. La argumentación que se desarrollará en este texto está enfocada en plantear cómo la actual ley de competencia desleal no será suficiente para juzgar comportamientos ejecutados en el mercado con intervención de IA. Para lograrlo, se comenzará por precisar el espacio en el que se deben ejecutar los comportamientos que son de interés para el régimen de competencia desleal. Hecho lo anterior, se procederá a mostrar algunos usos posibles de la IA para el desarrollo de actividades económicas dentro del mercado. Después, se desarrollarán tres estadios del juicio de competencia desleal en los que posiblemente se presentarán tres problemáticas que van a dificultar la aplicación de esta ley. Al final de este camino, el lector habrá conocido algunos

[*] Para citar este capítulo: http://dx.doi.org/10.15425/2017.574.

[**] Este capítulo refleja una postura personal basada en un ejercicio estrictamente académico.

presagios sobre lo que nos espera con el uso de IA en el mercado, específicamente en lo que tiene que ver con el futuro de nuestro actual régimen de competencia desleal.

La aplicación del régimen de competencia desleal a comportamientos realizados en el mercado

La aplicación del régimen de competencia desleal a situaciones concretas debe superar una serie de filtros que se conocen como ámbitos de aplicación. La utilidad de tales ámbitos radica en que, sin ellos, no es posible someter el caso a las normas que regulan la competencia desleal. En ese orden de ideas, no son estos los que determinan si una conducta es o no un acto de competencia desleal, pues esa finalidad la cumplen las normas que tipifican las diferentes conductas que el legislador ha considerado desleales y que se encuentran en los artículos 7 a 19 de la Ley 256 de 1996. En realidad, lo que determinan es si la situación que queremos someter a juicio puede ser estudiada a la luz del régimen de competencia desleal o si, por el contrario, esta no es de su interés y por tanto debería explorarse un régimen jurídico distinto.

Dichos ámbitos son tres: el objetivo, el subjetivo y el territorial, todos ellos regulados, respectivamente, en los artículos 2, 3 y 4 de la citada ley. Para efectos de este texto nos centraremos, en un primer momento, en el ámbito objetivo, específicamente en su doble exigencia, esto es, la necesidad de que el comportamiento se realice en el mercado y tenga fines concurrenciales, y más adelante, trabajaremos en el ámbito subjetivo.

De acuerdo con el artículo 2 de la ley de competencia desleal:

> Los comportamientos previstos en esta ley tendrán la consideración de actos de competencia desleal siempre que se realicen en el mercado y con fines concurrenciales. La finalidad concurrencial del acto se presume cuando este, por las circunstancias en que se realiza, se revela objetivamente idóneo para mantener o incrementar la participación en el mercado de quien lo realiza o de un tercero.

Tal como se infiere de esta norma, para que un comportamiento pueda ser analizado a la luz del régimen de competencia desleal debe cumplir dos requisitos. En primer lugar, debe *ser realizado en el mercado* y, en

segundo lugar, debe *tener finalidad concurrencial*. Por cuestiones metodológicas, en el siguiente apartado me ocuparé del primer requisito, y el segundo será abordado más adelante.

La realización del comportamiento en el mercado

No todos los escenarios en que las personas desarrollan sus distintos comportamientos resultan de interés para la aplicación del régimen de competencia desleal. Este pretende ser delimitado, de ahí que se encargue únicamente de aquellas acciones que se realizan en el *mercado*. Fernando Carbajo señala que "La ley se aplica, entonces, a prácticas comerciales realizadas públicamente en el mercado, quedando por fuera de su alcance los actos o prácticas meramente internos de las empresas u otras organizaciones"[1]. En tal sentido, escenarios distintos al del mercado —como serían los de las relaciones familiares, interpersonales, laborales, entre otros— no estarían incluidos como aquellos de interés para la ley de competencia desleal.

Para explicar lo anterior, pensemos, por ejemplo, que dos trabajadores aspiran a un ascenso en la compañía donde trabajan, razón por la cual han estado compitiendo de diversas formas a fin de demostrar sus capacidades y a partir de ello obtener esa mejor posición que ambos anhelan. En ese ejercicio, el aspirante 1 decide acudir donde el líder del área de Selección para contarle acerca de ciertos aspectos negativos del desempeño de su compañero. Dicha información, desafortunadamente, no correspondía con la realidad, pero fue contada de manera tan convincente que fue determinante para no conceder el ascenso al aspirante 2. Notemos que, en este caso, podríamos afirmar que existe una competencia entre dos personas, por cuanto se encuentran en una disputa sobre un objetivo común. Podríamos afirmar también que en medio de esta competencia uno de los participantes llevó a cabo un comportamiento que no se compadece con la lealtad, ya que faltó a la verdad para poder alcanzar el objetivo común. Todo ello podría llevarnos a

[1] Fernando Carbajo Cascón (coordinador), "La competencia desleal (I) Cláusula general e ilícitos por competencia desleal. La publicidad comercial desleal", en *Manual práctico de derecho de la competencia* (Valencia: Tirant Lo Blanch, 2017), 352.

afirmar, finalmente, que estamos frente a un caso en el que hubo una competencia desleal.

Sin embargo, ¿son ese tipo de comportamientos los que interesan a la ley de competencia desleal? La respuesta a este interrogante es no. Para precisarlo, profundicemos en el hecho de que el ámbito objetivo exige que los comportamientos sean *realizados en el mercado* para que puedan considerarse actos de competencia desleal, aspecto que implica tener claridad acerca de lo que es el mercado y lo que significa que un comportamiento se realice en él.

De acuerdo con Massaguer, el mercado es "un espacio institucional en el que se encuentran oferta y demanda, en el que se forman y desenvuelven las relaciones económicas"[2]. Por su parte, González precisa que "el mercado es una institución que facilita la interacción humana en el proceso de intercambio de bienes. El mercado, por tanto, va mucho más allá de la transacción de mercancías"[3]. Notemos de lo dicho por estos autores, que el mercado no corresponde a un espacio físico y, en esa medida, cuando se habla de realizar un comportamiento en el mercado no se está haciendo referencia a una acción que se ejecuta en un lugar al que acudamos "de cuerpo presente" para comercializar o adquirir productos y servicios.

Teniendo claro el concepto de *mercado*, resta establecer cuándo podemos entender que un comportamiento ha sido realizado en él. Para este propósito resultan valiosas las explicaciones de García Pérez, quien asegura que "para satisfacer el requisito es suficiente que el comportamiento ejerza (o pueda ejercer, añadimos nosotros) una influencia sobre las relaciones entre competidores o entre proveedores y clientes, es decir, que exista (o pueda existir, agregamos) un impacto sobre el mercado y la competencia económica"[4]. Lo dicho por García Pérez parece dejar claro lo que significa la realización en el mercado de un comportamiento; sin embargo, para la construcción de su explicación, afirma que "Se hace necesario dotar la expresión 'realizado en el mercado' de

[2] José Massaguer Fuentes, *Comentario a la ley de competencia desleal* (Madrid: Civitas, 1999), 120.

[3] Jorge Iván González, *Sentimientos y racionalidad en economía* (Bogotá: Universidad Externado de Colombia, 2016), 137.

[4] Rafael García Pérez, "El ámbito objetivo de aplicación de la ley de competencia desleal", *Derecho de los Negocios*, n.º 200 (2007): 10.

un sentido más aprehensible. Para ello nos ayudaremos de la aclaración que hace el Preámbulo de la Ley, que señala que el acto realizado en el mercado es aquel dotado de trascendencia externa"[5], lo cual no podemos trasladar al caso colombiano debido a que nuestra ley de competencia desleal no incluye el concepto de "trascendencia externa", que, sin mucha dificultad, permite comprender lo que significa la realización en el mercado de un comportamiento.

Pues bien, para salir de este embrollo, podemos acudir al objeto de la ley de competencia desleal contenido en su artículo 1, de acuerdo con el cual "[…] la presente ley tiene por objeto garantizar la libre y leal competencia económica, mediante la prohibición de actos y conductas de competencia desleal, en beneficio de todos los que participan en el mercado […]". Como se observa, la norma incluye como parte de su propósito el garantizar la libertad de competencia económica, haciéndolo en beneficio de todos los participantes del mercado, es decir, tanto de empresarios como de consumidores. Si esto es así, puede afirmarse válidamente que la ley de competencia desleal debe reprochar únicamente aquello que afecte, o pueda afectar[6], a la competencia y a los participantes del mercado, elementos todos que confluyen en un mismo escenario denominado *mercado*.

Siguiendo tal línea argumentativa, cabe dejar sentado, partiendo del contenido de nuestra ley de competencia desleal, que *un comportamiento se entiende realizado en el mercado cuando tiene, o puede tener, impacto en la competencia económica o en las relaciones entre empresarios y consumidores. Todo aquello que se encuentre por fuera de ese contexto no puede ser analizado a la luz del régimen de competencia desleal.*

Así, si retomamos el ejemplo propuesto, concluimos que a dicha situación no se le puede aplicar esta norma, por cuanto el comportamiento por juzgar, esto es, el haber hecho afirmaciones contrarias a la realidad para excluir del proceso de selección a un compañero de trabajo con el que se compite por una mejor posición laboral, no tiene ningún impacto sobre la competencia económica ni en las relaciones entre empresarios y

[5] *Ibid.*

[6] Téngase en cuenta que no es necesario que la afectación se produzca de manera efectiva, puesto que el régimen de competencia desleal puede activarse incluso frente a conductas desleales que aún no se han perfeccionado y frente a aquellas que, habiéndose perfeccionado, no han causado daño alguno (art. 20, Ley 256 de 1996).

consumidores, lo que lleva a concluir que se trata de un comportamiento realizado en un ámbito distinto al del mercado.

La inteligencia artificial en el mercado

En la obra de Miguel Cazorla *et al*. se define la inteligencia artificial, citando a Marvin Misky, como "la ciencia de construir máquinas para que hagan cosas que, si las hicieran los humanos, requerirían inteligencia"[7]. Por su parte, Alejandro Pazos *et al.* afirman que

> La IA es la rama de la ciencia que se encarga del estudio de la inteligencia en elementos artificiales y, desde el punto de vista de la ingeniería, propone la creación de elementos que posean un comportamiento inteligente. Dicho de otra forma, la IA pretende construir sistemas y máquinas que presenten un comportamiento que si fuera llevado a cabo por una persona, se diría que es inteligente. El aprendizaje, la capacidad de adaptación a entornos cambiantes, la creatividad, etc., son facetas que usualmente se relacionan con el comportamiento inteligente[8].

La IA ha tenido aplicación en diversos campos, como la medicina, la gestión y administración, las finanzas, las aplicaciones militares y espaciales, e incluso en el de las asesorías jurídicas. Gracias a ella se han logrado avances notables, pues el respaldo que brindan los sistemas y las máquinas con IA ha robustecido la capacidad de los seres humanos de obtener resultados positivos. En Colombia, por ejemplo, al revisar el registro de la oficina nacional de patentes[9] es posible encontrar la patente denominada "Silla de ruedas controlada por electrooculografía empleando una técnica de inteligencia artificial"[10], la cual está enmarcada

[7] Miguel Cazorla *et al*., *Fundamentos de inteligencia artificial* (Alicante: Publicaciones de la Universidad de Alicante, 1999), 2.

[8] Alejandro Pazos *et al*., "Inteligencia artificial y computación avanzada", en *Inteligencia artificial y computación avanzada,* editado por Juan Jesús Romero *et al*., (Santiago de Compostela: Fundación Alfredo Brañas, 2007), 10.

[9] SIC.

[10] Patente concedida mediante Resolución 11993 del 6 de mayo del 2019. Expediente NC2017/0006859.

en el campo de la electrooculografía. También es posible encontrar otras invenciones en trámite, como la denominada "Proceso de inteligencia artificial aplicado a una red neuronal de pronósticos de complicaciones de malaria", la cual está relacionada con el sector de la salud[11].

El mundo de los negocios no ha sido ajeno a estas bondades. Por ello, es posible encontrar actualmente diversas soluciones basadas en IA que son usadas por las compañías en el ejercicio de su concurrencia al mercado. Al respecto, para efectos de este artículo, es importante destacar que se han realizado desarrollos tecnológicos que permiten la interacción de los consumidores con los empresarios, pero a través de IA. Veamos algunos ejemplos:

- La compañía Aivo lanzó al mercado el producto denominado Voice, que ofrece una solución de atención al cliente. Este producto se encuentra en capacidad de entender las preguntas que le formulen los usuarios y ofrecerles una respuesta inmediata, a través de un canal de voz[12].
- El Banco Ciudad de Argentina utiliza chatbots de inteligencia artificial para atender a sus clientes. De acuerdo con información de Microsoft, el chatbot

> […] es una pieza de *software* que simula conversaciones reales, por eso permitirá responder las dudas más frecuentes de los usuarios como las asociadas a préstamos, cuentas, trámites, etc. La implementación de la solución de Intelligence Chat Bot Services basado en Microsoft Cognitive Services junto con la base de conocimientos de Microsoft Dynamics 365 le da acceso al Banco Ciudad a nuevos servicios cognitivos, basados en un conjunto de algoritmos que ayudan a procesar datos automáticamente para crear aplicaciones más personalizadas, que tienen

[11] Expediente NC2017/0008056 de la Superintendencia de Industria y Comercio de Colombia.

[12] "Presentan *call center* con inteligencia artificial", *El Nuevo Siglo,* 5 de abril del 2018, https://www.elnuevosiglo.com.co/articulos/04-2018-presentan-call-center-con-inteligencia-artificial.

por función entender las necesidades de los usuarios mediante la utilización de métodos naturales de comunicación[13].

- El Banco de Crédito del Perú cuenta con un asistente virtual llamado Arturito, destinado a la atención de sus clientes. De acuerdo con información de dicha compañía,

> Arturito es un BOT que opera con lo último de la tecnología de inteligencia (IA). Está preparado para responder todo tipo de preguntas alrededor de los temas que maneja. Pero, lo más interesante, es que su programa le permite aprender de cada nueva comunicación, por lo que su repertorio de respuestas se va incrementando mientras más se comunica con los usuarios[14].

Estos, que son solamente algunos de muchos ejemplos similares, nos muestran que, gracias a la IA, lo empresarios pueden ponerse en contacto con los consumidores e interactuar con ellos para resolver sus inquietudes, sin ninguna intervención de seres humanos, pues esa es una necesidad que las máquinas pueden suplir.

Es importante destacar que los sistemas con IA tienen la capacidad de aprender y de tomar decisiones a medida que van adquiriendo experiencia, para lo cual utilizan un algoritmo y la información que reciben de distintas fuentes. Luis Amador explica que

> Los investigadores en inteligencia artificial se ocupan del desarrollo e implementación de sistemas informáticos que generan resultados normalmente asociados con la inteligencia humana. Es decir, se apunta a la aplicación de una serie de cualidades como son la comprensión, *el*

[13] "Banco Ciudad: Innovación e inversión tecnológica para liderar la transformación digital", *News Center Microsoft Latinoamérica*, 30 de agosto del 2017, https://news.microsoft.com/es-xl/banco-ciudad-innovacion-e-inversion-tecnologica-liderar-la-transformacion-digital/.

[14] "Arturito, El BOT de BCP al servicio de nuestros clientes", *BCP*, acceso el 11 de noviembre del 2019, https://www.viabcp.com/blog-bcp/arturito-bcp.

> *aprendizaje*, el conocimiento, *la toma de decisiones*, la percepción, la creación, el razonamiento, etc. […][15]. [Énfasis añadido]

En tal sentido, es posible que los sistemas con IA que interactúan con consumidores, a medida que tienen más contacto con ellos, adquieran mayor habilidad para dar respuesta a las preguntas que formulan.

En consecuencia, resulta claro que los avances actuales en materia de IA permiten a los empresarios usarla para concurrir al mercado a fin de interactuar con los interesados en adquirir productos y servicios, esto es, los consumidores. Asumiendo la veracidad de esta afirmación, debemos llegar a la primera conclusión de este texto, consistente en que *Todo comportamiento realizado en el escenario del mercado (con finalidad concurrencial[16]) haciendo uso de IA es susceptible de ser analizado a la luz de las normas sobre competencia desleal.* Es importante que el lector tenga en cuenta esta conclusión, por cuanto es el punto de partida de las problemáticas que a continuación se van a plantear.

Tres problemáticas en torno a la aplicación del régimen de competencia desleal cuando se utiliza inteligencia artificial en el mercado

Pese a que la primera conclusión propuesta señala que los comportamientos ejecutados en el mercado haciendo uso de IA resultan de interés para la LCD, lo cierto es que los pasos subsiguientes a ella no parecen ser tan sencillos. Lo anterior, si tenemos en cuenta que a pesar de parecer evidente la aplicación de las normas sobre lealtad en la competencia a tales casos, hay un camino largo que se debe recorrer antes de calificarse un comportamiento como desleal. A continuación, se plantearán tres problemáticas, todas ellas encaminadas a vaticinar algunas dificultades a las que nos podríamos enfrentar cuando en Colombia abunde el uso de IA para efectos de concurrir al mercado.

[15] Luis Amador Hidalgo, *Inteligencia artificial y sistemas expertos* (Córdoba: Servicios de Publicaciones de la Universidad de Córdoba, 1997), 27.

[16] Este elemento del ámbito objetivo será explicado en el siguiente apartado.

La finalidad concurrencial[17]

Como se mencionó, para que un comportamiento pueda ser analizado bajo la LCD debe realizarse en el mercado y tener *finalidad concurrencial*, aspecto del que paso a ocuparme puesto que se trata de un concepto que no se encuentra definido en la ley.

Una primera aproximación la ofrece el inciso segundo del artículo 2 de la ley de competencia desleal, en el que, si bien no se define la finalidad concurrencial, al menos se establecen las circunstancias en las cuales se puede presumir que esta existió en un comportamiento. Según esa norma, cuando un comportamiento, apreciado objetivamente, resulta idóneo para mantener o incrementar la participación en el mercado de la persona que lo realiza, o de un tercero, se entiende que existió una finalidad concurrencial. Pero, como ya se dijo, esto no define tal figura, solo establece una presunción. Para De la Cruz,

> […] la finalidad concurrencial viene a complementar el acto que se realiza en el mercado, al darle sentido, por cuanto le exige que se dirija hacia la consecución de un fin comercial, "mantener o incrementar la participación en el mercado de quien lo realiza o de un tercero", más allá de una finalidad puramente personal[18].

La Real Academia Española define *finalidad*[19] como "Fin con que o por qué se hace algo", mientras que *fin* es el "objeto o motivo con que se ejecuta algo"[20]. Trasladando esto a lo que aquí interesa, diríamos que la finalidad corresponde al objeto o motivo por el cual la persona que ejecutó la conducta reprochada como desleal lo hizo. Si el motivo consistió en buscar el aseguramiento o la mejora de su participación en el

[17] Sobre la finalidad concurrencial se puede consultar también el artículo de mi autoría titulado "El proceso por actos de competencia desleal: Una materia en construcción", publicado en *Derecho procesal: Nuevas tendencias* (Bogotá: Instituto Colombiano de Derecho Procesal, 2020), 975.

[18] Dionisio Manuel de la Cruz Camargo, *La competencia desleal en Colombia: Un estudio sustantivo de la ley* (Bogotá: Universidad Externado de Colombia, 2014), 23.

[19] RAE, *Diccionario de la lengua española*, 23.ª ed., *s. v.* "finalidad", https://dle.rae.es/?w=finalidad&m=form

[20] *Ibid*., *s. v*. "fin", https://dle.rae.es/?w=fin&m=form.

mercado o la de un tercero, diríamos que la finalidad de quien realizó la conducta fue concurrencial.

Llegados a este punto es importante hacer claridad en que la *finalidad concurrencial* no puede definirse como la idoneidad objetiva de un acto para mantener o incrementar la participación en el mercado de quien lo realiza o de un tercero, como erróneamente podría pensarse si se malinterpretara la presunción del artículo 2 de la ley de competencia desleal. La finalidad concurrencial, como se explicó, corresponde a un aspecto subjetivo relacionado con el motivo que tuvo el autor del comportamiento al realizarlo. En este punto, la presunción desempeña un papel fundamental, ya que, si el comportamiento se revela objetivamente idóneo para mantener o incrementar la participación en el mercado de quien lo realizó o de un tercero, diríamos que se ejecutó con "finalidad concurrencial", pero no porque sea esa su definición, sino porque cuando un acto se ejecuta en las condiciones que menciona la norma, se presume, por disposición legal, que el autor lo hizo con ese propósito.

En tal sentido, lo que el legislador hizo en el inciso segundo del artículo 2 de la citada ley no fue definir la finalidad concurrencial, sino liberar al demandante de la carga de demostrar el elemento subjetivo subyacente a la comisión de la conducta, estableciendo para ello una presunción. Esta última puede ser desvirtuada por quien es demandado en el proceso de competencia desleal, para lo cual debe demostrar que su finalidad no era la de mantener o incrementar su participación o la de un tercero en el mercado, sino que se trataba de una finalidad distinta, pensemos por ejemplo en una estrictamente altruista o asociada al activismo social.

Ubicados en este escenario y retomando la idea de que todo comportamiento realizado en el mercado haciendo uso de IA es susceptible de ser analizado a la luz de las normas sobre competencia desleal, surge la necesidad de verificar si, además del requisito de haber sido realizado en el mercado, ese tipo de comportamientos cumplen también con el de la finalidad concurrencial.

Pues bien, esta será una de las primeras problemáticas que habremos de enfrentar cuando deba aplicarse el actual régimen de competencia desleal a comportamientos ejecutados en el mercado haciendo uso de IA, ya que no será fácil establecer la finalidad concurrencial. Para explicarlo, recordemos que las máquinas dotadas de IA pueden aprender y

tomar decisiones, aspecto que se advierte determinante de todo lo que nos depara con este avance tecnológico.

El Parlamento Europeo profirió en el 2017 una resolución con recomendaciones destinadas a la Comisión sobre Normas de Derecho Civil sobre Robótica, en la que se pueden leer consideraciones que destacan esa característica. El documento contiene, entre otras, las siguientes afirmaciones, que resultan pertinentes para el objeto de este artículo:

> G. Considerando que, a largo plazo, la tendencia actual que apunta al desarrollo de máquinas inteligentes y autónomas, con capacidad de ser entrenadas para pensar y tomas decisiones de manera independiente, no solo implica ventajas económicas, sino también distintas preocupaciones relativas a sus efectos directos e indirectos en el conjunto de la sociedad.
>
> […]
>
> R. Considerando que el desarrollo de toma de decisiones automatizadas y basadas en algoritmos y su creciente utilización incidirán sin duda en las elecciones de los particulares (por ejemplo, empresas o usuarios de internet) y de las autoridades administrativas y judiciales u organismos públicos de otro tipo, a la hora de tomar su decisión final, ya sea de carácter comercial, de ejercicio de la autoridad pública o de consumo; considerando que es necesario integrar salvaguardias y la posibilidad de control y verificación por parte de las personas en los procesos de toma de decisiones automatizados y basados en algoritmos.
>
> […]
>
> AA: Considerando que la autonomía de un robot puede definirse como la capacidad de tomar decisiones y aplicarlas al mundo exterior, con independencia de todo control o influencias externos; que esa autonomía es puramente tecnológica y que será mayor cuanto sea mayor el grado de sofisticación con que se haya diseñado el robot para interactuar con su entorno[21].

El Parlamento, tras hacer diversas consideraciones, pide a la Comisión proponer definiciones europeas comunes de *sistema ciberfísico*,

[21] http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_ES.html#title1, acceso, 13 de noviembre del 2019.

sistema autónomo, *robot autónomo inteligente* y sus distintas subcategorías, teniendo en cuenta algunas características de los robots inteligentes, entre ellas, su capacidad de autoaprendizaje a partir de la experiencia y la interacción, y su capacidad de adaptar su comportamiento y acciones al entorno.

Partiendo de esa idea, es decir, del hecho de que las máquinas cuenten con la capacidad, no solo de aprender, sino también de tomar decisiones frente a situaciones concretas, surge la necesidad de preguntarnos si detrás de cada "decisión" puede existir una "finalidad" o, mejor aún, una "finalidad concurrencial". Veamos el planteamiento en un ejemplo.

Un consumidor se encuentra en búsqueda de un modelo de zapatos específico que le ha resultado difícil conseguir, por lo que ha decidido comunicarse directamente con algún fabricante que los haga a su medida, lo que lo lleva a comunicarse con la fábrica que comercializa zapatos bajo la marca Benjamín Hernández.

Por error, el consumidor se comunicó con un fabricante distinto, que comercializa zapatos bajo la denominación Benjamín Fernández. Este último cuenta con un centro de atención de potenciales clientes que funciona con IA, el cual recibió la llamada. Cuando el consumidor preguntó si le contestaban de la fábrica Benjamín Hernández, la máquina que lo atendió, diseñada para ofrecer y vender productos, le respondió que era lo mismo. Gracias a ello, el consumidor decidió contratar la elaboración de sus zapatos con la fábrica Benjamín Fernández, bajo la idea equivocada de estar haciéndolo con Benjamín Hernández.

El ejemplo propuesto muestra la ejecución de un comportamiento que, al menos en principio, no resulta deseable debido a que se indujo a error al consumidor acerca del origen empresarial de los zapatos que compraría. Ese comportamiento fue *realizado en el mercado* por cuanto tuvo injerencia en la decisión de uno de sus participantes, esto es, el consumidor. ¿Pero podremos, con la misma facilidad, señalar que existió *finalidad concurrencial*?

No parece fácil concluir que el empresario era quien buscaba mantener o incrementar su participación en el mercado mediante la inducción a error a los consumidores. La razón para afirmarlo es que, siendo la finalidad concurrencial un elemento subjetivo, debería poderse atribuir al empr0esario, pero lo cierto es que el ejemplo sugiere que la máquina, a fin de lograr la venta del producto, fue quien causó un efecto perjudicial al consumidor. En el hecho de actuar de esa

forma, con el propósito de vender, no parece haber participado el empresario, puesto que el centro de atención de potenciales clientes funcionaba enteramente con IA.

Ahora bien, podría plantearse que la finalidad concurrencial en este tipo de casos aparece desde el hecho mismo de implementarse IA para el desarrollo de una actividad económica, bajo el entendido de que, precisamente, aquella se utiliza para mejorar las prestaciones económicas y, con ello, la posición dentro del mercado. Esta postura, sin embargo, no nos saca del todo del problema.

En efecto, si se tratara de un caso en el que el empresario adquirió las máquinas con IA y las entrenó deliberadamente para que cometieran conductas reprochables, como la confusión o el engaño a los consumidores, *con el fin de mantener o mejorar su posición en el mercado*, resultaría viable atribuirle, sin muchas dificultades, el fin concurrencial en la ejecución de esos comportamientos.

No obstante, el panorama sería menos claro en un escenario en el que se adquieren las máquinas para ofrecer y comercializar productos y servicios en condiciones transparentes y comercialmente aceptables, pero es la máquina la que de manera autónoma decide ejecutar acciones que afectan a los consumidores o a los competidores con tal de lograr importantes ventas. No es descabellado plantear esta posibilidad, ya que situaciones como esa pueden ocurrir sin que ni siquiera estemos frente a una falla en el funcionamiento de la IA. Explica Ercilla que

> […] en el ámbito de los daños causados por los robots, aparece una peculiaridad propia, que viene de la mano de lo que, observando las notas definitorias del "robot inteligente", podría denominarse "acción autónoma del robot en sentido estricto", o "*culpa in singularitatem*", que puede definirse como aquella acción causante de un daño y llevada a término por un robot como resultado de su forma de razonamiento y aprendizaje, sin que se detecte un fallo en su programación y/o diseño, y que además resulte impredecible según esta programación y/o diseño[22].

[22] Javier Ercilla García, *Normas de derecho civil y robótica, robots inteligentes, personalidad jurídica, responsabilidad civil y regulación* (España: Editorial Arazandi, 2018), 72.

Si es ese el escenario al que debemos enfrentarnos, difícilmente podría atribuirse finalidad concurrencial al empresario que adquirió una máquina dotada de IA con el propósito de mejorar su participación dentro del mercado, cuando es ella quien ejecuta una acción negativa de forma autónoma (en sentido estricto), por cuanto no ha sido entrenada deliberadamente para eso y, aun así, lo hizo. En esa medida, la acción de la máquina fue contraria al propósito que tuvo el empresario cuando tomó la decisión de implementar IA para el desarrollo de sus negocios y, desde ese punto de vista, el elemento subjetivo no aparece por ninguna parte.

Así, ante la dificultad de encontrar finalidad concurrencial atribuible al empresario cuando este utiliza IA en el desarrollo de su actividad económica, a lo que nos vamos a enfrentar es a la imposibilidad de someterlo a un juicio de competencia desleal por cuanto no habría forma de cumplir con el ámbito objetivo; en consecuencia, el caso no sería susceptible de ser analizado bajo la Ley 256 de 1996.

Una forma de superar este problema la encontraríamos en la posibilidad de atribuir finalidad concurrencial, no al empresario sino a las máquinas, en aquellos casos en los que el comportamiento del empresario y el de la IA son independientes debido a la decisión autónoma de esta última, lo que, en principio, permitiría someterla a juicio. Esto nos lleva hasta un tema de importancia, en lo que tiene que ver con la IA, que ha sido el de los daños causados por las máquinas, especialmente por la falta de claridad acerca de quién se debe considerar responsable de causarlos y, por tanto, quién debería indemnizar a la víctima. Tal circunstancia puede resultar particularmente difícil cuando nos encontramos frente a máquinas que tienen la capacidad de tomar decisiones de manera autónoma. Según explica Martin Ebers

> […] se constata que la creciente automatización ha conducido al resultado de que las actividades que al ordenamiento jurídico tradicionalmente le sirven como criterio para la imputación, se desplazan, paso por paso, del usuario al sistema. Puesto que el comportamiento de la máquina se determina cada vez menos desde una programación fijada de antemano y depende cada vez más de su interacción con el entorno, y el entorno respectivo a su vez genera procesos de aprendizaje y nuevas formas de comportamiento del sistema, surgen zonas ampliadas de acción de las máquinas que ya no pueden ser reducidas a determinadas cadenas de

> acciones. Más bien se trata de procesos que no están precisamente fijados en su desarrollo y que cada vez menos se pueden controlar durante el funcionamiento[23].

De tal suerte que las máquinas que toman decisiones de forma autónoma son motivo de atención en lo que a responsabilidad civil se refiere.

Para afrontar esta situación, una propuesta que ha hecho eco ha sido la de crear una personalidad jurídica específica para los robots. Al respecto, el Parlamento Europeo, en la resolución del 2017, pidió a la Comisión sobre Normas de Derecho Civil sobre Robótica analizar y considerar

> […] crear a largo plazo una personalidad jurídica específica para los robots, de forma que como mínimo los robots autónomos más completos puedan ser considerados personas electrónicas responsables de reparar los daños que puedan causar, y posiblemente aplicar la personalidad electrónica a aquellos supuestos en los que los robots tomen decisiones autónomas inteligentes o interactúen con terceros de forma independiente[24].

Bajo esta figura de una personalidad jurídica especial para los robots, podríamos superar el problema de la atribución de finalidad concurrencial a las máquinas dotadas de IA, por cuanto podríamos afirmar que la tienen cuando toman decisiones de manera autónoma, aunque su propósito no sea el de mantener o incrementar su participación en el mercado sino la de un tercero, que es el empresario que la utiliza en beneficio de su empresa. Empero, el ámbito objetivo no es suficiente para aplicar la ley de competencia desleal a un caso concreto, ya que una vez superado este debemos proceder a analizar el denominado "ámbito subjetivo", que nos plantea un nuevo problema.

[23] Martin Ebers, "La utilización de agentes electrónicos inteligentes en el tráfico jurídico: ¿Necesitamos reglas especiales en el derecho de la responsabilidad civil?". *InDret, Revista para el Análisis del Derecho*, n.º 3 (2016): 8-9.

[24] Parlamento Europeo, acceso el 13 de noviembre del 2019, http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_ES.html#title1.

El ámbito subjetivo

El ámbito subjetivo constituye el segundo filtro para la aplicación de la ley de competencia desleal. Al respecto, el artículo 3 de la Ley 256 de 1996 señala que "Esta ley se le aplicará tanto a los comerciantes como a cualesquiera otros participantes del mercado. La aplicación de la ley no podrá supeditarse a la existencia de una relación de competencia entre el sujeto activo y el sujeto pasivo en el acto de competencia desleal". Así, entonces, es el ámbito subjetivo lo que nos permite saber a qué personas se les puede aplicar el régimen de competencia desleal.

Observemos que la norma tiene una redacción bastante amplia, por tanto, son varias las personas que podrían ser sometidas a juicio de competencia desleal. En primera medida se habla de los "comerciantes". El Código de Comercio colombiano los define en su artículo 10 señalando que "son comerciantes las personas que profesionalmente se ocupan en alguna de las actividades que la ley considera mercantiles […]". Al respecto, Castro de Cifuentes señala que este calificativo

> […] se predica entonces de quienes realizan tales actos de manera habitual y no de manera esporádica. Los que ejecuten en forma estable actividades no mercantiles, como las profesiones liberales, aunque lo hagan en forma organizada, no son comerciantes y no les son aplicables las distintas consecuencias jurídicas derivadas de ese estatus[25].

Partiendo de este concepto es válido pensar que, por regla general, los implicados en un juicio de competencia desleal son los comerciantes, puesto que al ser ellos quienes acuden con frecuencia al mercado a ofrecer sus productos y sus servicios, son también los más expuestos a cruzar las líneas del ejercicio de la libre competencia económica, lo que finalmente los puede llevar a caer en el escenario de la deslealtad. Sin embargo, no son los únicos destinatarios de la ley de competencia desleal, ya que, además de los comerciantes, se aplica también a "cualesquiera otros participantes del mercado". Esta expresión permite incluir a todo aquel que concurra al mercado, aunque no lo haga de

[25] Marcela Castro de Cifuentes, *Derecho comercial: Actos de comercio, empresas, comerciantes y empresarios* (Bogotá: Editorial Temis, 2013), 154.

manera habitual o profesional, como ocurriría, por ejemplo, con quien esporádicamente vende un producto, o con los consumidores quienes también son participantes del mercado y por tanto destinatarios de la ley de competencia desleal.

Partiendo de estas explicaciones, aun cuando lográramos superar el ámbito objetivo en el caso de las máquinas que toman decisiones de manera autónoma, superar el ámbito subjetivo no sería un problema menor, puesto que resultaría difícil considerar a las máquinas como uno de los sujetos mencionados en el artículo 3 de la Ley 256 de 1996.

Para explicarlo, retomemos que dicha norma se aplica tanto a los comerciantes como a todas aquellas personas que sean participantes del mercado. En tal sentido, si las máquinas dotadas de IA se encuentran al servicio de un empresario que la ha adquirido y puesto en funcionamiento para el mejoramiento de sus prestaciones, parece difícil afirmar que dicha máquina es participante del mercado, cuando lo cierto es que no es más que un sofisticado instrumento que contribuye al mejor desarrollo de una empresa.

En efecto, la participación en el mercado implica acudir a él ya sea para ofrecer y comercializar un producto o un servicio, o ya sea para adquirirlo. Sin embargo, la máquina, aun cuando pudiera ejecutar comportamientos que impacten en ese escenario y lo hiciera de manera autónoma, lo haría al estar al servicio de un ser humano que es aquel empresario que ha decidido implementar IA en el desarrollo de su actividad económica. De tal suerte que la máquina, aun alcanzando un importante grado de autonomía, no gozaría de total independencia, pues su existencia misma en el escenario del mercado se debería a la decisión de un ser humano de ponerla allí.

De hecho, el artículo 22 de la ley de competencia desleal representaría un gran obstáculo frente a este tipo de situaciones, por cuanto establece que "si el acto de competencia desleal es realizado por trabajadores u otros colaboradores en el ejercicio de sus funciones y deberes contractuales, las acciones previstas en el artículo 20 de esta Ley, deberán dirigirse contra el patrono". Eso, en un escenario de IA, nos llevaría a la imposibilidad de someter a juicio a las máquinas debido a que, siendo ellas las colaboradoras del empresario, la demanda debería ser dirigida contra este.

En suma, si bien la postura que pregona por la creación de una personalidad jurídica especial para las máquinas nos ayudaría a cumplir

con el ámbito objetivo, no parece ser muy útil para verificar el cumplimiento del ámbito subjetivo, puesto que resulta válida para solucionar problemas de atribución, pero no para la determinación de la calidad de comerciante o de participante del mercado de un sujeto.

La exigencia de buena fe objetiva a las máquinas

La libre competencia económica es un derecho que, en Colombia, goza de consagración constitucional[26]. Como expliqué en un texto anterior, se concibe desde una doble dimensión

> […] pues es un derecho individual y al mismo tiempo es un derecho colectivo. Desde su dimensión individual, debe generar al empresario la posibilidad de obtener lucro a partir de su actividad económica, y desde su dimensión colectiva […], debe generar beneficios al consumidor con bienes y servicios de mejor calidad, con mayores garantías y a un precio real y justo[27].

Este, como por regla general ocurre, no es un derecho de carácter absoluto y por tanto es posible encontrar que tiene diversas limitaciones, siendo una de ellas el régimen de competencia desleal.

Según el artículo 1.º de la ley de competencia desleal: "la presente Ley tiene por objeto garantizar la libre y leal competencia económica,

[26] El artículo 333 de la Constitución colombiana señala que "La actividad económica y la iniciativa privada son libres, dentro de los límites del bien común. Para su ejercicio, nadie podrá exigir permisos previos ni requisitos, sin autorización de la ley. La libre competencia económica es un derecho de todos que supone responsabilidades. La empresa, como base del desarrollo, tiene una función social que implica obligaciones. El Estado fortalecerá las organizaciones solidarias y estimulará el desarrollo empresarial. El Estado, por mandato de ley, impedirá que se obstruya o se restrinja la libertad económica y evitará o controlará cualquier abuso que personas o empresas hagan de su posición dominante en el mercado nacional. La ley delimitará el alcance de la libertad económica cuando así lo exija el interés social, el ambiente y el patrimonio cultural de la Nación".

[27] José Fernando Sandoval Gutiérrez, "Medidas cautelares innominadas en procesos de competencia desleal y su capacidad de afectación a los consumidores", *Revista Vniversitas*, n.º 69 (2020).

mediante la prohibición de actos y conductas de competencia desleal, en beneficio de todos los que participen en el mercado […]". Conforme a ello, el régimen fue creado como un mecanismo de garantía de la libre y leal competencia económica, propósito que se logra gracias a la tipificación de una serie de comportamientos que según el legislador son actos de competencia desleal y pueden ser reprochados judicialmente. Para explicarlo, revisemos que una de las conductas que se consideran desleales es la "comparación". Señala el artículo 13 de la ley:

> […] se considera desleal la comparación pública de la actividad, las prestaciones mercantiles o el establecimiento propios o ajenos con los de un tercero, cuando dicha comparación utilice indicaciones o aseveraciones incorrectas o falsas, u omita las verdaderas. Así mismo, se considera desleal toda comparación que se refiera a extremos que no sean análogos ni comprobables.

Para explicar el acto de comparación

> […] es fundamental señalar que la comparación de prestaciones y establecimientos no es en sí misma un comportamiento desleal. Tal como pasa con varios de los artículos de la LCD, lo que se reprocha son las circunstancias en que se realiza. En el caso de la comparación desleal, esta es motivo de reproche cuando en el ejercicio comparativo se utiliza información que de alguna manera no corresponda con la realidad, por ejemplo cuando se utiliza información falsa, se incurre en imprecisiones o simplemente se omite la verdad[28].

Observemos que mediante el ejercicio del derecho a la libre competencia económica es posible concurrir al mercado a fin de buscar clientela y así obtener beneficios económicos. Esto incluye la posibilidad de ofrecer públicamente el producto o el servicio que se pretende comercializar e incluso confrontarlo con productos y servicios semejantes con el

[28] José Fernando Sandoval Gutiérrez, "La represión de la competencia desleal como mecanismo indirecto de protección al consumidor", en *Derecho del consumo: Tras un lustro del Estatuto del Consumidor en Colombia*, coordinado por Juan Francisco Ortega Díaz, Juan Carlos Martínez Salcedo y Gloria Isabel Osorio Giammaria (Bogotá: Ediciones Uniandes y Editorial Temis, 2018), 294.

objetivo de destacarlos por encima de los comercializados por los demás participantes del mercado. Sin embargo, ese derecho, por no ser absoluto, encuentra como límite la lealtad en la competencia. De ahí que se reproche como desleal la comparación pública que se lleva a cabo utilizando información que no se compadezca con la realidad.

A riesgo de ser reiterativo, revisemos otra de las conductas establecidas en la ley de competencia desleal. El artículo 11 de dicha norma señala que "se considera desleal toda conducta que tenga por objeto o como efecto inducir al público a error sobre la actividad, las prestaciones mercantiles o el establecimiento ajenos". Sobre esta conducta, señala Kresalja que

> […] muchos participantes en la lucha concurrencial creen que es más fácil y rentable aunque sea incorrecto, introducir productos u ofrecer servicios en el mercado haciendo uso de determinadas técnicas de sugestión para orientar la preferencia de los consumidores, técnicas que no hacen mención a factores esenciales como la calidad y el precio; esas conductas impiden la transparencia en el mercado, que solo puede alcanzarse cuando la información es veraz y pertinente. A través de los actos de engaño se trata de difundir o utilizar indicaciones susceptibles de inducir a error sobre las ventajas realmente obtenidas, queriendo hacer aparecer como verdadero lo que es falso[29].

Al igual que ocurría en el caso anterior, a pesar de las libertades de que gozamos gracias a la libre competencia económica, en el ejercicio de este derecho no es posible captar clientela utilizando medios que generen ideas en los destinatarios de la información que no correspondan con la realidad. La información usada en el ejercicio de la comercialización de productos y servicios debe ser transparente para que la decisión de quien los adquiere sea clara y esté libre de vicios.

En suma, aunque exista la libre competencia económica como un derecho, se establecieron también unas normas sobre lealtad que limitan su ejercicio. Esto impone el deber, a los titulares del derecho, de ejercerlo respetando ciertos parámetros de conducta, especialmente en lo que a

[29] Baldo Kresalja R., "Comentarios al Decreto Ley 26122 sobre represión de la competencia desleal", *Revista Derecho PUCP*, n.º 47 (1993), 55-56.

competencia desleal se refiere: la denominada buena fe objetiva. Emparanza expone que "El recurso a la buena fe objetiva permite residenciar la antijuridicidad del acto en la vulneración de las normas de conducta emanadas del principio de buena fe, entendido como límite funcional al derecho de desarrollar libremente una actividad en el mercado"[30].

Nuestro sistema de competencia desleal se encuentra cimentado sobre el deber de los participantes del mercado de actuar de buena fe. Pero no se trata de una buena fe asociada a aspectos subjetivos de quien ejecuta la conducta, sino de una buena fe que se analiza prescindiendo de ellos y que, más bien, tiene que ver con los deberes de conducta exigibles a quienes acuden al mercado. De ahí que se hable de una buena fe objetiva. Este deber de conducta lo encontramos explícito en el artículo 7 de la ley de competencia desleal, que corresponde a la denominada "cláusula general", en la que se establece que "Quedan prohibidos los actos de competencia desleal. Los participantes en el mercado deben respetar en todas sus actuaciones el principio de la buena fe comercial […]". Barona afirma, trabajando este mismo tema, que

> […] el concepto de buena fe contemplado en la norma no es psicológico, normalmente identificado con la ignorancia o error disculpable o excusable, sino objetivo, esto es, un modelo de conducta socialmente aceptable y exigible que impone determinados deberes de actuación y ciertos límites al ejercicio de los derechos y facultades a quienes operan en el mercado. De ahí que haya que integrarse la norma a través de unos modelos de conducta cuya infracción convierte en desleal la competencia, teniendo presente que la finalidad de la Ley no es otra que proteger la competencia en interés de todos los que participan en el mercado […][31].

Así pues, el artículo 7 de la ley de competencia desleal contiene el deber general de actuar de buena fe aplicable a todo aquel que concurra

[30] Alberto Emparanza Sobejano, "Competencia desleal y protección de los consumidores", en *Derecho de la competencia y cuestiones de actualidad*, dirigido por Luis María Miranda Serrano y Julio Costas Comesaña, coordinado por José Manuel Serrano Cañas y Antonio Casado Navarro (Madrid: Marcial Pons, 2018), 99.

[31] Silvia Barona Vilar, *Competencia desleal: Tutela jurisdiccional (especialmente proceso civil) y extrajurisdiccional* (Valencia: Tirant Lo Blanch, 2008), 295.

al mercado y que corresponde básicamente al estándar de conducta exigible a todos los participantes en él.

Pero el legislador no llegó únicamente hasta esa consagración general de la buena fe objetiva, ya que a partir del artículo 8 hasta el 17 consagró una serie de comportamientos que se consideran actos de competencia desleal, los cuales no son nada distinto a estándares definidos de comportamiento cuya contravención da lugar a la configuración de una conducta ejecutada contrariando la buena fe y, por consiguiente, un acto de competencia desleal. En sentido similar afirma Darnaculleta:

> La técnica jurídica utilizada tradicionalmente para la regulación de la competencia desleal en los países de nuestro entorno jurídico toma como punto de partida una cláusula general en la que se prohíbe este tipo de competencia, seguida de una enumeración de supuestos concretos de aplicación de esta prohibición. La prohibición general opera, así, de forma subsidiaria, con el objeto de expulsar del mercado las prácticas no previstas expresamente, bien por su carácter marginal o extraño, bien por la aparición de nuevos comportamientos incorrectos derivados de la continua evolución de las prácticas comerciales[32].

Para resumir, la libre competencia económica, como derecho que no tiene carácter absoluto, encuentra como uno de sus límites el régimen de competencia desleal, que se encuentra cimentado sobre el deber de buena fe objetiva que deben respetar todos los participantes del mercado.

Retornando al escenario en el que las máquinas dotadas de IA toman decisiones de manera autónoma y suponiendo además que logramos atribuirles finalidad concurrencial, así como superar el ámbito subjetivo de alguna forma, ¿podríamos dar el siguiente paso para afirmar que las conductas ejecutadas por ellas en el mercado, con fines concurrenciales, podrían ser calificadas como actos de competencia desleal?

Este, a mi juicio, corresponde al siguiente problema con el que podríamos encontrarnos a la hora de aplicar la ley de competencia desleal. Lo anterior, si tenemos en cuenta que dicho régimen se erige como una forma de limitar un derecho, esto es, el derecho a la libre competencia

[32] M. Mercè Darnaculleta I Gardella, *La competencia desleal* (Madrid: Iustel, 2007), 39.

económica. En tal sentido, el deber de actuar en el mercado de acuerdo a los parámetros de la buena fe objetiva solamente es exigible a quienes ejercen ese derecho.

Si esto es así, la buena fe objetiva no es exigible a las máquinas dotadas de IA, por cuanto, al menos en la actualidad, no son titulares de ningún derecho, lo que incluye, por supuesto, el derecho a la libre competencia económica. Al no serlo, tampoco sería posible exigirles actuar dentro de los límites de ese derecho, lo que en otras palabras significa que las máquinas no pueden ser juzgadas de acuerdo con la ley de competencia desleal, bajo el entendido de que no les es imponible el estándar de la buena fe objetiva.

Valga agregar para finalizar que este inconveniente no se superaría con la creación de una personalidad jurídica especial para las máquinas, pues esa figura no está pensada para convertirlas en titulares de todo tipo de derechos. Sobre el punto, Díaz Alabart señala que

> La personalidad jurídica específica para los robots, que podemos denominar personalidad electrónica, no debería ser otra cosa que una capacidad jurídica bastante limitada en razón a su objetivo indemnizatorio ya señalado. No se trataría de hacer a los robots inteligentes sujetos de derechos de forma general, sino que con esa personalización limitada se eliminarían algunos problemas para que se pueda hacer efectiva la indemnización por los daños causados[33].

Es decir que esta figura ha sido pensada dentro del ámbito de la responsabilidad civil como una solución para garantizar que se indemnicen los perjuicios causados por las máquinas, pero no para convertirlas definitivamente en sujetos de derechos. Superar el inconveniente impondría la necesidad de ampliar la cobertura de la personalidad jurídica especial, hasta un punto que permita exigir a las máquinas dotadas de IA los deberes correlativos al derecho de libre competencia económica.

Es así como nuestra actual ley de competencia desleal, en la forma en que está diseñada, resultará insuficiente para juzgar comportamientos ejecutados en el mercado con intervención de IA, lo que impone la

[33] Silvia Díaz Alabart, *Robots y responsabilidad civil* (Madrid: Reus, 2018), 77.

necesidad de reflexionar anticipadamente, para que los robots, que en realidad son una solución, no se conviertan en un problema más.

Conclusiones

Todo comportamiento realizado en el escenario del mercado usando IA es susceptible de ser analizado a la luz de las normas sobre competencia desleal. Sin embargo, hay al menos tres problemáticas que dificultarían su aplicación, las cuales tendrían lugar en tres estadios distintos.

La dificultad de encontrar finalidad concurrencial atribuible al empresario cuando este utiliza IA en el desarrollo de su actividad económica podría impedir someterlo a un juicio de competencia desleal por cuanto no habría forma de cumplir con el "ámbito objetivo"; en consecuencia, el caso no podría analizarse bajo la Ley 256 de 1996.

Aunque superáramos los problemas asociados al ámbito objetivo, al analizar el ámbito subjetivo encontraríamos dificultad en afirmar que las máquinas dotadas de IA pueden tener la calidad de participantes del mercado.

El estándar de comportamiento de "buena fe objetiva" no es exigible a las máquinas dotadas de IA pues no son titulares del derecho a la libre competencia económica, lo que impide imponerles actuar dentro de los límites de aquel.

Bibliografía

Alabart Díaz, Silvia. *Robots y responsabilidad civil*. Madrid: Reus, 2018.

"Arturito, el BOT de BCP al servicio de nuestros clientes". Acceso el 11 de noviembre del 2019. https://www.viabcp.com/blog-bcp/arturito-bcp.

"Banco Ciudad: Innovación e inversión tecnológica para liderar la transformación digital". *News Center Microsoft Latinoamérica,* 30 de agosto del 2017. https://news.microsoft.com/es-xl/banco-ciudad-innovacion-e-inversion-tecnologica-liderar-la-transformacion-digital/.

Barona Vilar, Silvia. *Competencia desleal: Tutela jurisdiccional (especialmente proceso civil) y extrajurisdiccional*. Valencia: Tirant Lo Blanch, 2008.

Carbajo Cascón, Fernando. "La competencia desleal (I). Cláusula general e ilícitos por competencia desleal: La publicidad comercial desleal". En *Manual*

práctico de derecho de la competencia, coordinado por Fernando Carbajo Cascón. Valencia: Tirant Lo Blanch, 2017.

Castro de Cifuentes, Marcela. *Derecho comercial: Actos de comercio, empresas, comerciantes y empresarios*. Bogotá: Editorial Temis, 2013.

Darnaculleta i Gardella, M. Mercè. *La competencia desleal.* Madrid: Iustel, 2007.

De la Cruz Camargo, Dionisio Manuel. *La competencia desleal en Colombia: Un estudio sustantivo de la ley.* Bogotá: Universidad Externado de Colombia, 2014.

Ebers Martin. "La utilización de agentes electrónicos inteligentes en el tráfico jurídico: ¿Necesitamos reglas especiales en el derecho de la responsabilidad civil?". *InDret, Revista para el Análisis del Derecho*, n.º 3 (2016).

Emparanza Sobejano, Alberto. "Competencia desleal y protección de los consumidores", en *Derecho de la competencia y cuestiones de actualidad*, dirigido por Luis María Miranda Serrano y Julio Costas Comesaña, coordinado por José Manuel Serrano Cañas y Antonio Casado Navarro, 95-106. Madrid: Marcial Pons, 2018.

Ercilla García, Javier. *Normas de derecho civil y robótica, robots inteligentes, personalidad jurídica, responsabilidad civil y regulación.* España: Editorial Arazandi, 2018.

García Pérez, Rafael. "El ámbito objetivo de aplicación de la ley de competencia desleal". *Derecho de los Negocios*, n.º 200 (2007): 7-18.

González, Jorge Iván. *Sentimientos y racionalidad en economía.* Bogotá: Universidad Externado de Colombia, 2016.

Hidalgo, Luis Amador. *Inteligencia artificial y sistemas expertos*. Córdoba: Servicios de Publicaciones de la Universidad de Córdoba, 1997.

Kresalja R., Baldo. "Comentarios al Decreto Ley 26122 sobre represión de la competencia desleal". *Derecho PUCP*, n.º 47 (1993): 13-86.

Massaguer Fuentes, José. *Comentario a la ley de competencia desleal.* Madrid: Civitas, 1999.

Miguel Cazorla, Patricia Compañ, Francisco Escolano y Ramón Rizo. *Fundamentos de inteligencia artificial.* Alicante: Publicaciones de la Universidad de Alicante, 1999.

Parlamento Europeo. Acceso el 13 de noviembre del 2019. http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_ES.html#title1.

Pazos, Alejandro, Nieves Pedreira, Juan Ramón Rabuñal y Javier Pereira. "Inteligencia artificial y computación avanzada". En *Inteligencia artificial y computación avanzada,* editado por Juan Jesús Romero, Carlos Dafonte,

Ángel Gómez y Fernando Jorge Penousal (pp. 9-34). Santiago de Compostela: Fundación Alfredo Brañas, 2007.

"Presentan *call center* con inteligencia artificial". *El Nuevo Siglo*, 5 de abril del 2018. https://www.elnuevosiglo.com.co/articulos/04-2018-presentan-call-center-con-inteligencia-artificial

Sandoval Gutiérrez, José Fernando. *Derecho procesal: Nuevas tendencias*. Bogotá: Instituto Colombiano de Derecho Procesal, 2014.

— "Medidas cautelares innominadas en procesos de competencia desleal y su capacidad de afectación a los consumidores". *Revista Vniversitas*, n.º 69 (2020).

— "La represión de la competencia desleal como mecanismo indirecto de protección al consumidor". En *Derecho del consumo: Tras un lustro del Estatuto del Consumidor en Colombia*, coordinado por Juan Francisco Ortega Díaz, Juan Carlos Martínez Salcedo y Gloria Isabel Osorio Giammaria, 283-302. Bogotá: Ediciones Uniandes y Editorial Temis, 2018.

Superintendencia de Industria y Comercio (SIC). Expediente NC2017/0006859.

— Expediente NC2017/0008056.

Capítulo IV

Sandboxes regulatorios: un enfoque innovador para la regulación de las *FinTechs*[*]

Catalina Guío Español

Introducción

En los últimos años, el sector de los servicios financieros se ha visto perturbado por la aparición de nuevas tecnologías financieras (*FinTechs*) y modelos de negocio (*TechFins*) que buscan la innovación y la competitividad. Sin embargo, en un entorno posterior a la crisis financiera, en el que la regulación se ha visto como una forma de gestionar los riesgos y asegurar la estabilidad, esta evolución tecnológica plantea un importante reto regulatorio: ¿cómo promover la innovación, manteniendo la estabilidad financiera y protegiendo a los consumidores?

Para resolver esta pregunta, los reguladores tienen tres formas diferentes de abordar las *FinTechs* y los *TechFins*: (1) el *enfoque estándar*, en el que se exige a los desarrolladores de *TechFins* y *FinTechs* que cumplan con el marco regulatorio general, sin normas ni requisitos especiales; (2) el *enfoque colaborativo*, que permite a estas empresas probar nuevas tecnologías en un entorno controlado seguro, proporciona licencias temporales, concede exenciones y otorga flexibilidad caso por caso; y (3) el *enfoque personalizado*, que adopta un nuevo marco regulatorio que establece límites para estas actividades y los entrantes en el mercado.

Los países que adoptan un enfoque colaborativo de la innovación han promovido la creación de "*sandbox* regulatorios", que se conocen como espacios seguros de experimentación, en los que se pueden probar nuevas tecnologías e ideas de negocio, sin estar sujetas a requisitos

[*] Para citar este capítulo: http://dx.doi.org/10.15425/2017.575.

o repercusiones regulatorias. Este enfoque fue desarrollado por el Reino Unido y está ganando importancia en Estados Unidos y en los países de Asia-Pacífico como una forma de abordar los desafíos planteados por las *FinTechs*.

Así las cosas, en este capítulo me propongo desarrollar una mejor comprensión de lo que es un *sandbox* regulatorio, en qué se diferencia de otros enfoques regulatorios, así como los beneficios y riesgos de utilizar este enfoque para la regulación de *FinTechs*. Además, busco estudiar los *sandboxes* regulatorios establecidos hasta ahora en esta industria, incluyendo los casos de Reino Unido, Singapur y Australia, con el propósito de identificar sus características comunes, sus principales retos y sus resultados. Todo ello me ayudará a proponer un marco para el desarrollo de estos espacios experimentales en otros países en el futuro.

Enfoques reguladores de las tecnologías financieras

Uno de los principales objetivos de la regulación financiera es proteger la integridad y la estabilidad del sistema financiero, promoviendo la seguridad y la solidez de las instituciones financieras[1]. Además, los reguladores financieros tienen el mandato de "proteger a los consumidores e inversores contra el fraude y luchar contra la evasión fiscal, el blanqueo de dinero y la financiación del terrorismo, asegurando que los riesgos se entienden y gestionan a fondo"[2].

Hoy en día, el rápido cambio y la entrada de nuevos participantes en el sector financiero han creado nuevas oportunidades de innovación y crecimiento. Sin embargo, el desarrollo de tecnologías disruptivas —que tienen el potencial de servir mejor a los consumidores— se ve condicionado

[1] Svein Andresen, "Regulatory and Supervisory Issues from FinTech", acceso el 20 de octubre del 2019, http://www.fsb.org/wp-content/uploads/Cambridge-Centre-for-Alternative-Finance-Regulatory-and-Supervisory-Issues-from-FinTech.pdf.

[2] Christine Lagarde, "A Regulatory Approach to FinTech", *FMI*, acceso el 23 de octubre del 2019, https://www.imf.org/external/pubs/ft/fandd/2018/06/how-policymakers-should-regulate-cryptoassets-and-fintech/straight.htm.

por la incertidumbre regulatoria, que afecta no solo a las empresas FinTech, sino también a las instituciones financieras tradicionales[3].

Ante el riesgo regulatorio, las empresas *FinTech* y los operadores tradicionales tienen dos alternativas: "Salir del mercado por completo u operar en una zona gris [...]. Una empresa puede no estar dispuesta a ofrecer un nuevo producto porque teme que su(s) regulador(es) vea(n) negativamente la novedad del producto, aunque este sea totalmente conforme"[4]. Por lo tanto, la incertidumbre y el miedo a la regulación impiden la innovación y la competencia.

En un entorno tan cambiante, las autoridades financieras se enfrentan al reto de apoyar las disrupciones innovadoras y, al mismo tiempo, velar por la estabilidad financiera y garantizar la protección de los consumidores. Para ello, los reguladores han adoptado tres enfoques normativos diferentes.

El enfoque estándar

En este enfoque, los operadores tradicionales y los nuevos están obligados a cumplir con la estructura reguladora existente. Desde el punto de vista del regulador, puede aplicarse de dos maneras diferentes: (1) de forma pasiva, al mejor estilo *laissez-faire*, permitiendo a los participantes en el mercado probar sus nuevos productos o servicios sin repercusiones inmediatas por parte del regulador —como era el caso de China antes del 2015—[5]; (2) o de forma agresiva, persiguiendo a las empresas para que cumplan con el entorno estrictamente regulado.

Este es el enfoque de la mayoría de las jurisdicciones hasta la fecha[6]. Aunque puede proteger contra los riesgos —en su forma más agresiva—, también puede restringir la innovación y dar lugar a la desprotección

[3] Dan Quan, "Here's What the CFPB's Sandbox Should Look Like", *American Banker*, 13 de septiembre del 2018, https://www.americanbanker.com/opinion/heres-what-the-cfpbs-sandbox- should-look-like.

[4] Quan, "What the CFPB's Sandbox".

[5] Douglas Arner *et al*., "FinTech and RegTech: Enabling Innovation While Preserving Financial Stability", *Georgetown Journal of International Affairs* 18, n.º 3 (2017): 47-58, doi:10.1353/gia.2017.0036.

[6] *Ibid.*

de los consumidores, al arbitraje regulatorio e incluso al fraude —en su estilo más pasivo—.

El enfoque colaborativo

Con este enfoque, los reguladores pretenden crear un entorno normativo más flexible para que se desarrollen nuevas competencias. Caso por caso, las empresas *FinTech* y las entidades financieras tradicionales están obteniendo licencias condicionadas y excepciones parciales para probar sus productos o servicios en un entorno estrechamente supervisado.

Los *sandboxes* regulatorios son una parte fundamental de este enfoque. Se han concebido como espacios seguros en los que las empresas pueden probar nuevos servicios financieros y modelos de negocio basados en la tecnología, en un entorno en vivo pero controlado, sin tener que someterse a un proceso completo de autorización y licencia[7]. A estas empresas se les permite experimentar en un espacio bien definido y durante un periodo limitado.

El propósito de este enfoque

> […] no es desregular el mercado, ni dar un cheque en blanco a los innovadores; de hecho, es todo lo contrario [...]. La admisión en el recinto de seguridad es una razón significativa para que las nuevas empresas salgan de la sombra y para que los incumbentes exploren ideas innovadoras sin temer que eso afecte a la supervisión de su negocio actual[8].

De este modo, los *sandboxes* abordan el problema de la incertidumbre regulatoria para los innovadores, al tiempo que permiten a los reguladores conocer los últimos avances de las *FinTechs*, influir en ellos y garantizar que se tengan en cuenta las consideraciones regulatorias[9]. Por

[7] Financial Conduct Authority. *Regulatory Sandbox,* acceso el 23 de octubre del 2019, https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf, 1.

[8] Jason Henrichs, "FinTech Needs More Regulatory 'Sandboxes'", *American Banker*, 26 de abril del 2018, https://www.americanbanker.com/opinion/fintech-needs-more-regulatory- sandboxes.

[9] Andresen, "Regulatory and Supervisory Issues".

lo tanto, los *sandboxes* se han convertido en espacios de colaboración entre los reguladores, los operadores tradicionales y los nuevos participantes del sector de los servicios financieros.

El enfoque personalizado

Con este enfoque, se espera que los reguladores adopten un nuevo marco normativo para las *FinTechs*, que contemple requisitos más adecuados y equilibrados para los nuevos participantes, así como para el desarrollo de nuevas actividades[10]. Se estima que este nuevo conjunto de normas y políticas será el resultado de las lecciones aprendidas por los reguladores durante el proceso de experimentación del *sandbox*.

Hasta ahora, este ha sido el enfoque en diferentes jurisdicciones en relación con temas específicos como el *crowdfunding*, los préstamos entre particulares y las ofertas públicas de criptomonedas.

Sandboxes regulatorios alrededor del mundo

Tal y como ya se estableció, los *sandboxes* regulatorios permiten a los innovadores de servicios financieros probar sus nuevas soluciones en un entorno controlado, exento de la regulación financiera existente, pero supervisado de cerca por las autoridades financieras.

Debido a los múltiples beneficios de este enfoque regulatorio —que incluyen la reducción de costes en la exploración de nuevos modelos e ideas de negocio, la mejora de la protección de los consumidores y el intercambio activo de información—, numerosas jurisdicciones están promoviendo la creación de *sandboxes* regulatorios para estimular las innovaciones *FinTech*.

En este apartado, describiré los *sandboxes* reguladores del Reino Unido, Singapur y Australia, identificando sus principales características y herramientas.

[10] Arner *et al*., "FinTech and RegTech".

Reino Unido

El *sandbox* regulatorio del Reino Unido fue la primera iniciativa de este tipo que se puso en marcha. Fue anunciada por la Autoridad de Conducta Financiera (FCA por sus siglas en inglés) en noviembre del 2015 y entró en vigor a partir de junio del 2016, cuando se abrió a recibir las solicitudes[11].

Para ser aceptadas en el *sandbox*, las empresas deben presentar una solicitud en la que expongan el cumplimiento de los siguientes criterios de elegibilidad[12]:

- *Ámbito de aplicación*. La nueva solución prevista debe estar diseñada para llevarse a cabo o apoyar el negocio de los servicios financieros en el mercado del Reino Unido.
- *Innovación genuina*. La nueva solución deberá ser novedosa o significativamente diferente a las ofertas existentes en el mercado.
- *Beneficio identificable para el consumidor*. La innovación debe ofrecer un beneficio identificable para los consumidores, ya sea directa o indirectamente —por medio de una mayor competencia—. En este punto deben identificarse los riesgos para el consumidor, así como las propuestas para su mitigación. En cualquier caso, este criterio debe seguir cumpliéndose a lo largo de todo el periodo de pruebas del *sandbox*.
- *Necesidad de un* sandbox. La empresa debe tener una necesidad real de probar la innovación en un marco de *sandbox*, lo que significa que las pruebas en vivo son necesarias para la pregunta que la empresa necesita responder. Las razones para necesitar un *sandbox* incluyen, pero no se limitan a: (1) la innovación no encaja fácilmente en el marco regulatorio existente, lo que hace difícil o costoso introducir la solución en el mercado, (2) no hay medios alternativos para realizar la prueba fácilmente sin el apoyo de la

[11] Financial Conduct Authority, *Regulatory Lessons Learned Report,* acceso el 23 de octubre del 2019, https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf, 4.

[12] Financial Conduct Authority, *Regulatory Sandbox*, 7.

FCA, y (3) el proceso de autorización completo sería demasiado costoso/difícil para una prueba de viabilidad corta.
- *Listo para la prueba*. La empresa debe tener un plan de pruebas bien desarrollado, con objetivos, parámetros y criterios de éxito claros. Los recursos para llevar a cabo la prueba deben estar probados, y deben existir salvaguardias adecuadas para los clientes, así como medidas para una reparación apropiada, en caso de ser necesario.

Las solicitudes se realizan dos veces al año por cohortes. Una vez que son admitidas, las empresas pueden disponer de una de las siguientes herramientas[13]:

- *Autorización restringida*. Proceso adaptado que permite a las empresas recibir autorización para probar sus nuevos servicios o productos según lo acordado con la FCA. Los requisitos de autorización son proporcionales a las actividades de prueba, por lo que el trámite es más rápido y menos costoso que el de una autorización completa.
- *Exenciones de normas*. Cuando está claro que las actividades de prueba no cumplen una norma de la FCA, y se demuestra que su cumplimiento es excesivamente gravoso, la FCA puede eximir o modificar la norma para efectos de la prueba.
- *Orientación individual*. Cuando no está claro cómo se aplican las normas a la empresa, la FCA puede emitir una orientación individual en el contexto de la prueba específica. Esto daría a la empresa la seguridad de que la FCA no tomaría medidas contra ella.
- *Cartas de no aplicación*. En aquellos casos en los que no son aplicables ni las exenciones ni las orientaciones individuales, la FCA puede emitir cartas de no aplicación si considera que las actividades de prueba no infringen sus requisitos ni perjudican sus objetivos. Estas cartas solo se aplican durante la duración de la prueba y no limitan la responsabilidad de la empresa hacia sus consumidores.

[13] *Ibid*., 8-9.

Estas herramientas están diseñadas para facilitar el examen de los solicitantes. Sin embargo, no siempre son necesarias. Por lo tanto, su uso dependerá de las características de la empresa y del producto o servicio que se vaya a ofrecer.

Las empresas que prueban en el *sandbox* del Reino Unido son, en su mayoría, *start-ups* del sector de la banca, que requieren una autorización restringida. Además, la FCA ha detectado que los participantes suelen probar la aplicación de nuevas tecnologías a productos o servicios tradicionales, en lugar de la creación de productos totalmente nuevos. De las tecnologías empleadas, la de registro distribuido (DLT, por sus siglas en inglés) es la más popular entre las empresas. Otros participantes importantes son las empresas de nueva creación que desarrollan soluciones para los sectores de los seguros generales[14].

El *sandbox* del Reino Unido ha demostrado ser un éxito. Alrededor del noventa por ciento de las empresas que completaron las pruebas están trabajando para conseguir un lanzamiento al mercado más amplio, y la mayoría de ellas ha pasado a conseguir una autorización completa. Además, la participación en el *sandbox* ha reducido el tiempo y los costes de entrada en el mercado de estas empresas, ya que la comunicación constante con el asesor de la FCA les ha ayudado a comprender mejor el marco normativo, lo que ha reducido los gastos en consultores externos. En ese mismo sentido, experimentar en el *sandbox* ha facilitado el acceso a la financiación de las empresas, debido a la certeza que este tipo de enfoque aporta a los inversores. Por último, este enfoque normativo de las tecnologías financieras también ha permitido a la FCA trabajar con los participantes en el *sandbox* "para desarrollar salvaguardias de protección del consumidor en los nuevos productos y servicios"[15].

Singapur

La versión singapurense del *sandbox* regulatorio se introdujo en junio del 2016, cuando la Autoridad Monetaria de Singapur (MAS, por sus siglas en inglés) reconoció que "ante circunstancias en las que no está

[14] Financial Conduct Authority, *Regulatory Lessons Learned Report*, 8-9.

[15] *Ibid*., 5-6.

tan claro si un nuevo producto o servicio financiero cumple con los requisitos legales y reglamentarios, algunas [instituciones financieras] o *start-ups*, pueden pecar de cautelosas y optar por no implementarlo"[16], lo que hace que se pierdan oportunidades de innovación en el sector de los servicios financieros. Por ello, el *sandbox* regulatorio se creó para fomentar la experimentación, de forma que las innovaciones prometedoras puedan probarse en el mercado y tengan la oportunidad de una mayor adopción.

Para acceder al *sandbox*, las empresas *FinTech* de Singapur y las ya existentes deben presentar una solicitud que cumpla los siguientes criterios de evaluación[17]:

- *Utilizar la tecnología de forma innovadora*. El servicio financiero propuesto deberá incluir tecnología nueva o emergente o utilizar la tecnología de forma innovadora. Los servicios financieros que son similares a los que ya se ofrecen no son elegibles.
- *Beneficio para los consumidores y/o la industria*. Los solicitantes deben demostrar cómo el servicio financiero aborda un problema o aporta beneficios a los consumidores o a la industria.
- *Despliegue en Singapur a mayor escala*. La empresa deberá tener la intención y la capacidad de desplegar la solución en Singapur a mayor escala después de realizar la prueba. Si esto no es posible —por ejemplo, porque no es comercialmente viable—, el participante deberá, en cualquier caso, seguir contribuyendo al desarrollo de la industria de servicios financieros en Singapur.
- *Escenarios de prueba claramente definidos y resultados esperados*. Los escenarios y los resultados esperados se determinarán por adelantado y se informará a la MAS de los progresos realizados según un calendario acordado.
- *Condiciones límite claramente definidas*. Las condiciones de experimentación deberán estar claramente definidas para que el

[16] Monetary Authority of Singapore, *FinTech Regulatory Sandbox Guidelines*, acceso el 22 de octubre del 2019, https://www.mas.gov.sg/-/media/MAS/Smart-Financial-Centre/Sandbox/FinTech-Regulatory-Sandbox-Guidelines-19Feb2018.pdf?la=en&hash=1F4AA49087F9689249FB8816A11AEAA6CB3DE833, 3.

[17] *Ibid*., 5.

interés de los consumidores y la seguridad y solidez de la industria estén siempre protegidos.
- *Evaluación y mitigación de los riesgos significativos*. Se fomenta la realización de pruebas preliminares para identificar los posibles riesgos y las medidas por adoptar para su mitigación.
- *Estrategia de salida y transición claramente definida*. Se debe presentar a la MAS una estrategia de salida y transición para aquellos casos en los que la solución propuesta tenga que interrumpirse o no pueda desplegarse a mayor escala.

Teniendo en cuenta el alcance de los criterios de evaluación, se espera que las empresas hayan realizado su propia debida diligencia sobre el servicio financiero que se va a ofrecer —incluidas las pruebas previas—, y que conozcan los requisitos reglamentarios para aplicar la innovación propuesta, antes de presentar la solicitud. Además, se espera que cumplan plenamente todos los requisitos legales y reglamentarios cuando salgan del *sandbox*, y tienen "la responsabilidad de garantizar que existe un plan para cumplir estos requisitos"[18].

No hay un periodo específico para que las empresas presenten las solicitudes. Una vez admitidas, las herramientas de experimentación se facilitan caso por caso. En este sentido, la MAS adopta un enfoque basado en el riesgo para determinar la forma más adecuada y eficaz de apoyo normativo. Aunque la MAS anuncia en sus directrices que este apoyo incluye "la flexibilización de los requisitos legales y reglamentarios específicos"[19], no se enumeran ni describen, ya que dependería del análisis de cada caso concreto.

La primera empresa que salió del *sandbox* regulatorio, en agosto del 2017, fue un corredor de seguros digital —PolicyPal— que permite a los clientes adquirir pólizas de seguros por medio de una aplicación[20].

[18] Monetary Authority of Singapore, *FAQs on FinTech Regulatory Sandbox*, acceso el 22 de octubre del 2019, https://www.mas.gov.sg/development/fintech/regulatory-sandbox.

[19] *Ibid*., 3-5.

[20] Monetary Authority of Singapore, "Experimenting in the Sandbox", acceso el 24 de octubre del 2019, http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/FinTech-Regulatory-Sandbox/Experimenting-in-the-sandbox.aspx.

En agosto del 2019, la MAS introdujo el "*Sandbox* Express" como complemento al enfoque del *sandbox* descrito. Con este mecanismo, las empresas que realizan las siguientes actividades: (1) llevar a cabo negocios como corredor de seguros, y (2) establecer u operar un mercado organizado, pueden experimentar con servicios o productos financieros innovadores en el mercado sin tener que pasar por la solicitud del *sandbox* existente. Esta aprobación rápida —en un plazo de veintiún días tras la solicitud a la MAS— está diseñada para la prueba de servicios y productos financieros que conllevan riesgos bajos y bien conocidos, y se basan en la divulgación a los clientes y en los informes continuos a la MAS[21].

Australia

El marco regulatorio australiano para el *sandbox*, establecido en el 2016 por la Comisión Australiana de Valores e Inversiones (ASIC, por sus siglas en inglés), ofrece tres opciones para que las empresas *FinTech* prueben sus nuevas soluciones, a saber:

- *Exenciones legales existentes o flexibilidad en la ley*. La legislación australiana prevé una serie de situaciones en las que no es necesario tener una licencia para prestar servicios financieros. Entre ellas se encuentran la actuación en nombre de un titular de licencia existente, los productos de pago en los que los pagos solo pueden realizarse a una persona y el crédito concedido a empresas o con fines comerciales.
- *La "exención de licencia para las empresas de tecnología financiera" de la ASIC*. Las empresas están legalmente autorizadas a probar determinados productos y servicios durante doce meses sin tener una licencia, si cumplen los requisitos de elegibilidad y siguen ciertas condiciones.
- *Exención individual de la ASIC*. Cuando ninguna de las otras dos soluciones es aplicable a la empresa, esta puede solicitar una

[21] Monetary Authority of Singapore, *Sandbox Express Guidelines*, acceso el 30 de octubre del 2019, https://www.mas.gov.sg/-/media/MAS/Smart-Financial-Centre/Sandbox-Express/Sandbox-Express-Guidelines-7-Aug.pdf?la=en&hash=E7917E9851BBE097AB7E889D64591FA340CC483C.

exención individual. Bajo esta figura, se permite a los innovadores probar un producto o servicio sin licencia en los términos acordados con la ASIC, previa solicitud y revisión.

Debido a la escasa participación en el *sandbox* (solo siete entidades desde su creación), en septiembre del 2020 la ASIC logró la modificación de la Ley de Sociedades y la Ley de Crédito con el fin de proporcionar exenciones de licencia condicionales para probar productos de servicios financieros y de crédito por medio de lo que se denominó el *sandbox* mejorado.

A diferencia de la primera versión, este nuevo *sandbox* permite no solo la participación de empresas locales o extranjeras —registradas en Australia— sin licencia, sino también que las empresas con licencia puedan probar nuevos servicios que actualmente no están autorizadas a proporcionar. También son elegibles para participar las personas naturales que sean ciudadanos australianos o residentes permanentes y que no estén autorizados para ejercer la actividad o prestar los servicios financieros que están probando[22].

La prueba sobre una actividad crediticia o un servicio financiero puede hacerse por una única vez, a un número ilimitado de clientes, durante máximo veinticuatro meses, con un límite de exposición de cinco millones de dólares australianos. Los participantes pueden utilizar el *sandbox* varias veces para probar diferentes servicios y actividades para los que no cuenten con una licencia y que no hayan probado ya[23].

Este *sandbox* mejorado, al igual que el anterior, solo permite la experimentación para ciertos productos financieros y sus servicios asociados, para los clientes *retail*. Para los mayoristas es posible realizar la prueba sobre cualquier producto financiero, excepto derivados y operaciones de financiación con reposición del margen. Los productos financieros que permiten experimentación en el *sandbox* incluyen depósitos, facilidades de pago no monetarias, productos de seguro general, seguros de vida y productos de jubilación[24].

[22] ASIC, "INFO 248 Enhanced Regulatory Sandbox", *ASIC*, https://asic.gov.au/for-business/innovation-hub/enhanced-regulatory-sandbox/info-248-enhanced-regulatory-sandbox/.

[23] ASIC, "INFO 248".

[24] ASIC, *Annual Report 574*, 7.

Para ser elegibles, los participantes deben ahora pasar dos pruebas: la del beneficio público neto y la de la innovación. Así, quienes deseen ingresar deben demostrar, por una parte, que el producto o servicio financiero aborda un problema actual para los consumidores o el mercado australiano, aumenta las posibilidades de elección de los consumidores del país, reduce los costos o brinda una mejor experiencia al usuario, o proporciona una mayor eficiencia. Por otra parte, los interesados deben demostrar por qué su servicio financiero o actividad propuesta es nueva o diferente a lo que existe en el mercado australiano[25].

Estos dos requerimientos son nuevos para el espacio controlado de pruebas australiano, y con ello se acercan a los *sandboxes* existentes en cuanto a exigir soluciones verdaderamente innovadoras, que cumplan con ciertos objetivos que el regulador ha fijado en pro del desarrollo de los mercados financieros y de los consumidores.

La aplicación al *sandbox* se hace mediante una notificación a la ASIC, frente a la cual esta autoridad puede pronunciarse dentro de los treinta días siguientes. Si no lo hace, se entiende que la excepción fue otorgada en los términos de la notificacion y comienza a correr el plazo para su prueba.

Desde la puesta en funcionamiento del *sandbox* mejorado a mayo del 2021, había cinco proyectos en experimentación, que incluían iniciativas innovadoras sobre medios de pago, inversiones y billeteras digitales[26].

Una propuesta de marco para el diseño de un *sandbox* regulatorio

El enfoque colaborativo de la regulación requiere la creación de espacios seguros para la experimentación. Estos espacios deben ofrecer suficiente flexibilidad para que los innovadores pongan a prueba sus soluciones, al tiempo que protegen a los consumidores y permiten una estrecha supervisión gubernamental. En este sentido, el éxito de estos espacios, así

[25] Australian Government Department of Treasury, "Enhanced Regulatory Sandbox", acceso el 24 de octubre del 2019, https://treasury.gov.au/consultation/c2017-t230052/.

[26] ASIC, "Enhanced Regulatory Sandbox Exemption Users", https://asic.gov.au/for-business/innovation-hub/enhanced-regulatory-sandbox/enhanced-regulatory-sandbox-exemption-users.

como los beneficios potenciales para los consumidores, los reguladores, los nuevos participantes y los incumbentes depende en gran medida de las características del diseño del espacio controlado de pruebas.

A partir de los casos estudiados, se puede establecer que los principales componentes de diseño de un *sandbox* regulatorio son los objetivos, los criterios de elegibilidad, el calendario y los costes, y las herramientas del *sandbox*.

Objetivos

Los principales objetivos del *sandbox* regulatorio son definidos por los reguladores según su mandato y establecidos en los instrumentos diseñados para su creación. Los objetivos comunes a todos los *sandboxes* regulatorios estudiados incluyen

- Promover la competencia efectiva en los servicios financieros regulados.
- Fomentar y facilitar la innovación.
- Garantizar que la regulación de los nuevos productos y servicios sea adecuada y eficaz y promueva la confianza de los inversores y consumidores.

Como puede verse, el objetivo de los reguladores de promover la competencia por medio de la innovación suele estar condicionado al mandato de proteger a los consumidores y la estabilidad del mercado.

Criterios de elegibilidad

Solo los productos y servicios que están bajo la autoridad del regulador pueden ser probados en el *sandbox* regulatorio. Sin embargo, depende de cada regulador determinar quién puede participar. Los participantes pueden incluir solo a los incumbentes, solo a las *start-ups*, o a ambos.

De los casos estudiados se desprende que debe fomentarse la participación de ambos (incumbentes y nuevos participantes). La búsqueda de eficiencias por medio de la innovación no es en absoluto exclusiva de las nuevas *FinTechs*. Por lo tanto, para promover la competencia en

condiciones equitativas, los *sandboxes* regulatorios deben estar abiertos a todos los participantes del mercado.

Otros criterios relativos a los participantes son el número máximo de clientes atendidos, la exposición de los clientes y los productos y servicios ofrecidos. Estas limitaciones permiten establecer salvaguardias para la protección de los consumidores, como el refuerzo de la información, los requisitos de capital y los fondos de compensación[27]. Sin embargo, como se ha visto en el caso de Australia, estas restricciones también pueden limitar el número de empresas que entran en el *sandbox* y se benefician de él, razón principal por la cual debió ser totalmente reformado.

En cuanto a los productos y servicios que deben probarse en el *sandbox* regulatorio, todas las jurisdicciones estudiadas parecen estar de acuerdo en que deben cumplir los siguientes criterios:

- Auténtica innovación. Ser significativamente diferente de otras ofertas del mercado, ya sea utilizando la tecnología o no.
- Beneficiar a los consumidores y/o a la industria, ya sea directa o indirectamente.
- Estar preparados para las pruebas, esto es, que incluya escenarios de prueba claramente definidos y resultados esperados, así como pruebas previas.
- Identificar los riesgos importantes y las formas de mitigarlos.
- Tener una estrategia de salida y transición claramente definida.

Calendario y costes

Los reguladores parecen estar de acuerdo en que las nuevas soluciones se prueben en el *sandbox* solo durante un tiempo limitado. Una vez concluida la fase de experimentación, los innovadores deberán buscar una autorización para seguir ofreciendo sus productos o servicios financieros, o bien poner fin a sus actividades por completo.

[27] Ivo Jenik y Kate Lauer, "Regulatory Sandboxes and Financial Inclusion", *CGAP*, acceso el 24 de octubre del 2019, http://www.cgap.org/research/publication/regulatory-sandboxes-and-financial-inclusion, 3.

Sin embargo, cada regulador decide si este tiempo es fijo, como en el caso australiano, o se establece caso por caso, como en Singapur y el Reino Unido. Teniendo en cuenta que el tiempo fijo establecido por el regulador australiano ha resultado demasiado corto —como demuestran las modificaciones realizadas a este espacio, que lo amplían de uno a dos años—, un acuerdo sobre el tiempo entre el regulador y el participante parece servir mejor a los fines del *sandbox*.

Por otro lado, aunque la entrada en el *sandbox* suele ser gratuita, los reguladores deberán considerar si algunos costes administrativos de la tramitación y el estudio de la solicitud se trasladan a los consumidores. No obstante, deben tener cuidado para que esto no se convierta en una barrera de entrada para las pequeñas empresas nuevas.

Herramientas para el *sandbox*

La forma en que el regulador permite a los participantes entrar en el *sandbox* determina, en cierto modo, las herramientas de que disponen. Cuando se requiere un proceso de solicitud —como es el caso del Reino Unido y Singapur—, los participantes suelen disponer de las siguientes herramientas del *sandbox*:

- Autorización restringida
- Exenciones de las normas
- Orientación individual
- Cartas de no ejecución

Como cada caso particular se analiza antes de entrar en el *sandbox*, los reguladores pueden dar a las empresas las herramientas que mejor se ajustan a su proyecto de innovación y a su situación particular. Bajo esta estructura, se asigna a cada uno de los participantes un responsable del caso, con el fin de apoyar el diseño y la ejecución de la prueba. Tanto las empresas como los reguladores se benefician de la comunicación constante entre el funcionario y los innovadores: las empresas, al obtener las herramientas y la información necesaria en cada etapa del proceso de prueba; y el regulador, al obtener información detallada sobre cómo se están desarrollando los nuevos productos o servicios, ya sea para mejorar la protección del consumidor o para promover una mayor regulación.

En cambio, cuando existe una exención general, como en Australia, la empresa solo puede actuar sin la autorización requerida; por lo tanto, no se concede ninguna orientación ni retroalimentación por parte del regulador. Si uno de los objetivos del *sandbox* regulatorio es promover la colaboración para fomentar la innovación mediante el intercambio de ideas, esta podría no ser la mejor manera de hacerlo.

Las exenciones generales tienen el potencial de permitir que más empresas participen en el *sandbox*. No obstante, deben diseñarse de forma que solo puedan ofrecerse determinados productos o servicios, y se requieren limitaciones estrictas en cuanto a los clientes y la exposición para garantizar la protección del consumidor. Debido a estas restricciones, menos participantes de los esperados pueden beneficiarse de la exención general, por lo que su propósito puede verse socavado.

La Arenera: la caja de arena reguladora de la autoridad financiera colombiana

Siguiendo las tendencias establecidas por los reguladores financieros alrededor del mundo, en el 2018 la Superintendencia Financiera de Colombia (SFC) presentó el primer *sandbox* regulatorio en el país. En su diseño se puede identificar fácilmente el marco descrito, así:

- *Objetivos*. Facilitar la innovación sostenible y responsable en el sistema financiero[28].
- *Criterios de elegibilidad*. Abierto a todos los participantes del mercado. Sin embargo, las entidades que no están bajo la supervisión de la SFC no pueden probar productos o servicios que solo están legalmente permitidos a las instituciones financieras bajo la supervisión de la SFC. Además, el producto o servicio que se va a probar debe (1) ser una verdadera innovación tecnológica o una nueva forma de utilizar alguna tecnología existente; (2) tener un impacto o una relación tangible con el sector financiero;

[28] Superintendencia Financiera de Colombia, *Manual de funcionamiento la Arenera*, acceso el 5 de noviembre del 2019, https://www.superfinanciera.gov.co/descargas/institucional/pubFile1030976/manualarenera.pdf, 3.

(3) representar un beneficio o resolver un problema para el consumidor financiero, facilitar la inclusión financiera, desarrollar los mercados financieros o mejorar la competencia entre las entidades supervisadas por la SFC; y (4) justificar adecuadamente la necesidad de operar en el *sandbox* regulatorio[29].

- *Plazos y costes*. Los plazos se establecen caso por caso y la solicitud para entrar al espacio controlado de prueba es gratuita[30].
- *Herramientas* sandbox. La SFC puede adaptar sus instrucciones (incluidas en sus circulares) caso por caso, para que durante el periodo de prueba los participantes puedan aplicar instrucciones alternativas emitidas por esta autoridad[31].

Aunque la SFC incluye como una de las herramientas del *sandbox* la vigilancia constante para evitar la ejecución de actividades financieras no autorizadas, esta no es una herramienta que se les da a los participantes, sino un propósito que debe cumplir el propio *sandbox*. Por lo tanto, debería incluirse como uno de sus objetivos.

A diferencia de países como Reino Unido, Singapur y Australia, en Colombia el acceso al sistema financiero todavía es limitado. Es por ello que la Arenera privilegia como criterio de elegibilidad soluciones que faciliten la inclusión financiera y/o el desarrollo de mercados financieros. Esto también se evidencia en los productos y servicios que actualmente se están probando en el *sandbox*: a abril del 2021 había diez participantes, la mayoría de ellos probando productos que permitirán simplificar la forma en que los consumidores financieros acceden a las cuentas de depósito y a los fondos de inversión colectiva.

Durante el proceso de publicación de esta obra, el Gobierno nacional expidió el Decreto 1234 del 2020, por el cual se crea un espacio controlado de prueba para actividades propias de las entidades vigiladas por la SFC. Este nuevo *sandbox* regulatorio entrará a reemplazar a la Arenera una vez que la Superintendencia expida la regulación correspondiente.

[29] *Ibid*., 5-6.

[30] *Ibid.*, 2.

[31] *Ibid.*, 4.

Sin embargo, al igual que la Arenera, este nuevo espacio controlado de prueba puede ser analizado según el marco descrito en este artículo así:

- *Objetivos*. Aprovechar la innovación en los servicios y productos financieros, protegiendo al consumidor financiero y la integridad y estabilidad del sistema, además de prevenir arbitrajes regulatorios.
- *Criterios de elegibilidad*. Las entidades financieras o personas jurídicas que quieran acceder al *sandbox* deben presentar un desarrollo tecnológico innovador, para productos o servicios que se vayan a prestar en el territorio colombiano, que cumpla con alguna de las siguientes finalidades: (1) aumentar la eficiencia en los servicios y productos financieros, (2) resolver una problemática para los consumidores financieros, (3) facilitar la inclusión financiera, (4) mejorar el cumplimiento normativo, y/o (5) desarrollar los mercados financieros o mejorar su competitividad. El desarrollo tecnológico innovador deberá estar lo suficientemente avanzado para que pueda ser probado tan pronto se expida el certificado de operación temporal.
- *Plazos y costes*. La prueba podrá tener lugar por un plazo máximo de dos años, contados desde la expedición del certificado de operación temporal.
- *Herramientas* Sandbox. La SFC expedirá para las personas jurídicas que busquen convertirse en una entidad vigilada una autorización de constitución temporal, mientras que para las entidades vigiladas podrá expedir un certificado de operación temporal. El procedimiento para la constitución u operación temporal está todavía pendiente por definir por parte de la SFC.

A diferencia de la Arenera, este nuevo espacio controlado de prueba permitirá la revisión de la regulación expedida por el Ministerio de Hacienda y Crédito Público por medio de la Unidad de Regulación Financiera (URF). En esa medida, se amplía el espectro de la regulación que puede ser sujeto de modificación o excepción una vez terminada la prueba, pues ya no se limita a las instrucciones de la SFC mediante sus circulares, sino que incluye también los decretos reglamentarios.

Pese a lo anterior, el decreto no establece cuál es el procedimiento que se debe seguir en caso de que el desarrollo tecnológico innovador implique una modificación a la regulación vigente, lo que resulta especialmente preocupante respecto a las expectativas que puedan tener sus participantes. Tratándose de un *sandbox* regulatorio, lo mínimo que se podría esperar es una revisión de la regulación en adelante, con el fin de que los desarrollos tecnológicos innovadores producto de pruebas exitosas puedan seguir funcionando en caso de que así lo requieran.

Conclusiones

El crecimiento y desarrollo del sector de los servicios financieros depende de la innovación, sin embargo, este crecimiento tiene que ser sostenible y asegurar un riesgo mínimo para los consumidores. Los *sandboxes* regulatorios sugieren un enfoque que permite equilibrar todos estos objetivos, al mejorar el diálogo entre el regulador y la industria, uniéndolos a favor de los consumidores.

Los beneficios de este enfoque son múltiples. Desde el punto de vista del innovador, contar con un marco estandarizado y publicitado para tratar las innovaciones reduce la incertidumbre y el temor regulatorio; en consecuencia, también se reducen los costes y el tiempo para introducir las nuevas soluciones en los mercados. Gracias a la certidumbre y la orientación que proporciona este enfoque, las empresas *FinTech* tienen un mayor acceso a la financiación y —junto con los operadores tradicionales— dependen menos de asesores jurídicos externos. Menos riesgos se traducen en una reducción del ciclo de comercialización y un mayor retorno de la inversión.

Desde la perspectiva del regulador, este enfoque aporta transparencia al sistema financiero. La comunicación constante con los innovadores no solo facilita el aprendizaje, sino que también proporciona al regulador información suficiente para prevenir cualquier daño a los consumidores o a la estabilidad de los mercados. El hecho de que las soluciones se prueben en un entorno controlado permite al regulador establecer las salvaguardias adecuadas y actuar con prontitud cuando alguno de sus mandatos se vea comprometido. Además, una vez concluidas las pruebas, pueden surgir nuevas normas de regulación y supervisión personalizadas.

A pesar de lo anterior, también hay riesgos que deben abordarse para usar de manera adecuada este enfoque. Una mala selección de los participantes, los sesgos o la falta de transparencia pueden limitar el potencial del *sandbox*. Hay que establecer unos criterios de elegibilidad bien definidos para que todas las empresas compitan en igualdad de condiciones. El éxito del *sandbox* regulatorio depende de la reputación del regulador y de los participantes. Por lo tanto, es necesario establecer previamente los procedimientos de aplicación y darlos a conocer con todo detalle.

Además, para garantizar la confianza de los consumidores en el sistema y limitar las consecuencias de cualquier fallo en el proceso de pruebas, deben establecerse salvaguardias. Sin embargo, deben diseñarse de tal manera que no desalienten la participación en el *sandbox*.

Los elevados requisitos de capital, los fondos de compensación y las pólizas de seguro tienen el riesgo de actuar como barreras de entrada para las pequeñas empresas de nueva creación. La flexibilidad del *sandbox* permite al regulador equilibrar los objetivos de mejorar la competencia y promover la innovación con sus mandatos de protección del consumidor y estabilidad financiera. Las características de diseño de esta herramienta desempeñan un papel importante en este sentido; todas ellas —los objetivos, los criterios de elegibilidad, los plazos y costes, y las herramientas— deben estar alineadas para que se logre una innovación sostenible. En el cuadro IV.1 se resumen las características del diseño de los *sandboxes* regulatorios estudiados.

El éxito de este enfoque —medido en términos de mejora de la competencia y de la confianza de los consumidores e inversores— dependería de la capacidad del regulador para establecer unos criterios de elegibilidad que permitan seleccionar las mejores empresas y las innovaciones verdaderamente genuinas, así como de su capacidad para determinar un momento adecuado para la experimentación y para proporcionar las herramientas adecuadas para cada caso particular.

Cuadro IV.1. Características del diseño de los *sandboxes* regulatorios estudiados

Características del diseño	**Reino Unido**	**Singapur**	**Australia**
Objetivos	Promover la competencia efectiva en interés de los consumidores apoyando la innovación disruptiva.	Transformar Singapur en un centro financiero inteligente fomentando la adopción de tecnología innovadora y segura en el sector financiero.	• Fomentar y facilitar la innovación en los servicios financieros y el crédito cuando sea probable que produzca buenos resultados para los inversores y los consumidores financieros. • Garantizar que la regulación de los nuevos productos y servicios sea adecuada y eficaz, y promueva la confianza de los inversores y consumidores. • Garantizar que los mercados funcionen de manera justa y eficiente.
Criterios de elegibilidad	• Se permite la participación de los titulares y de los nuevos participantes. • Innovación destinada al mercado británico. • Innovación genuina. • Beneficio para el consumidor. • Necesidad de un *sandbox*. • Preparado para las pruebas.	• Abierto a instituciones financieras y empresas *FinTech* de nueva creación. • Utilizar la tecnología de forma innovadora. • Beneficios para los consumidores y/o la industria. • Despliegue en Singapur a mayor escala. • Escenarios de prueba claramente definidos y resultados esperados. • Condiciones de entorno claramente definidas. • Riesgos significativos evaluados y mitigados. Una estrategia de salida y transición claramente definida.	• La empresa que se acoja a la exención no debe tener prohibida la prestación de servicios financieros ni ser ya titular de una licencia de AFS o de crédito. • Los límites de los clientes y de la exposición. • Productos y servicios limitados.

Calendario y costes	• Duración limitada, aunque no se especifica. • Sin coste.	• La duración estará bien definida, pero no es fija. • Sin coste	• Doce meses • Tasas asociadas a la solicitud de ayuda individual.
Herramientas para el *sandbox*	• Autorización restringida. • Exenciones de las normas. • Orientación individual. • Cartas de no ejecución de medidas.	• Relajación de requisitos legales y reglamentarios específicos definidos caso por caso.	• Exención de licencia. • Alivio individual.

Fuente: Elaboración propia.

Bibliografía

Andresen, Svein. "Regulatory and supervisory issues from *FinTech*". Financial Stability Board. http://www.fsb.org/wp-content/uploads/Cambridge-Centre-for-Alternative-Finance-Regulatory-and-Supervisory-Issues-from-FinTech.pdf.

Arner, Douglas, Dirk Zetzsche, Ross Buckley y Janos Nathan Barberis. "FinTech and RegTech: Enabling innovation while preserving financial stability". *Georgetown Journal of International Affairs* 18, n.º 3 (2017): 47-58. doi:10.1353/gia.2017.0036.

ASIC. "Annual Report l 574". *ASIC*.

— "Enhanced regulatory sandbox exemption users". *ASIC*, https://asic.gov.au/for-business/innovation-hub/enhanced-regulatory-sandbox/enhanced-regulatory-sandbox-exemption-users.

— "INFO 248 enhanced regulatory sandbox". *ASIC*, https://asic.gov.au/for-business/innovation-hub/enhanced-regulatory-sandbox/info-248-enhanced-regulatory-sandbox/.

Australian Government Department of Treasury. "Enhanced regulatory sandbox", acceso el 24 de octubre del 2019. *Australian Government. The Treasury*. https://treasury.gov.au/consultation/c2017-t230052/.

Financial Conduct Authority. "Regulatory lessons learned report". *FCA*, acceso el 23 de octubre del 2019. https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf.

— "Regulatory Sandbox". *FCA*, acceso el 23 de octubre del 2019. https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf.

Henrichs, Jason. "FinTech needs more regulatory 'sandboxes'". *American Banker,* 26 de abril del 2018. https://www.americanbanker.com/opinion/fintech-needs-more-regulatory-sandboxes.

Jenik, Ivo y Kate Lauer. "Regulatory sandboxes and financial inclusion". *CGAP*, acceso el 24 de octubre del 2019. http://www.cgap.org/research/publication/regulatory-sandboxes-and-financial-inclusion.

Lagarde, Christine. "A regulatory approach to FinTech". *FMI*, acceso el 23 de octubre del 2019. https://www.imf.org/external/pubs/ft/fandd/2018/06/how-policymakers-should-regulate-cryptoassets-and-fintech/straight.htm.

Monetary Authority of Singapore. "Experimenting in the Sandbox". *MAS*, acceso el 24 de octubre del 2019. http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/FinTech-Regulatory- Sandbox/Experimenting-in-the-sandbox.aspx.

— "FAQs on FinTech Regulatory Sandbox". *MAS*, acceso el 22 de octubre del 2019. https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf.

— "FinTech Regulatory Sandbox Guidelines". *MAS*, consultado el 22 de octubre del 2019. https://www.mas.gov.sg/-/media/MAS/Smart-Financial-Centre/Sandbox/FinTech-Regulatory-Sandbox-Guidelines-19Feb2018.pdf?la=en&hash=1F4AA49087F9689249FB8816A11AEAA6CB3DE833.

— "Sandbox Express Guidelines". *MAS*, acceso el 30 de octubre del 2019. https://www.mas.gov.sg/-/media/MAS/Smart-Financial-Centre/Sandbox-Express/Sandbox-Express-Guidelines-7-Aug.pdf?la=en&hash=E7917E9851BBE097AB7E889D64591FA340CC483C.

Quan, Dan. "Here's what the CFPB's Sandbox should look like". *American Banker,* 13 de septiembre del 2018. https://www.americanbanker.com/opinion/heres-what-the-cfpbs-sandbox- should-look-like.

Superintendencia Financiera de Colombia. *Manual de funcionamiento de la Arenera*. *SFC*, acceso el 5 de noviembre del 2019. https://www.superfinanciera.gov.co/descargas/institucional/pubFile1030976/manualarenera.pdf.

Capítulo V

El determinismo algorítmico en Colombia: riesgos para la protección del usuario*

María Lorena Flórez Rojas

Introducción

La relatividad se aplica a la física, no a la ética.

Albert Einstein

En los últimos años, han salido al mercado diversas aplicaciones que argumentan utilizar inteligencia artificial (IA). Una de las más discutidas ha sido Clearview AI, fundada por el empresario australiano Hoan Ton-That. Esta empresa se basó en un método de raspado o *web scraping*, del cual obtuvo millones de imágenes de acceso público de las plataformas de redes sociales y las compiló en una base de datos de reconocimiento facial, la cual puso a disposición de las fuerzas policiales y la industria privada. Es importante resaltar que Clearview AI ha estado en medio del debate público, debido a las preocupaciones relacionadas con la protección de datos, la privacidad e incluso falsos perfilamientos[1]. Por su parte, agentes federales y estatales de Estados Unidos informaron que, si bien tenían un conocimiento limitado de cómo funciona el *software* de Clearview AI y quién está detrás de este, habían utilizado su aplicación

* Para citar este capítulo: http://dx.doi.org/10.15425/2017.576.

[1] Benjamin Sobel, "HiQ v. LinkedIn, Clearview AI, and a New Common Law of Web Scraping", *SSRN Electronic Journal* (19 de mayo del 2020), https://doi.org/10.2139/ssrn.3581844; Donna Lu, "Face up to reality", *New Scientist* 245, n.º 3267 (1.º de febrero del 2020): 23, https://doi.org/10.1016/s0262-4079(20)30212-8.

para ayudar a resolver casos de hurto, robo de identidad, fraude con tarjetas de crédito, asesinato y explotación sexual infantil[2].

De igual forma, en el 2015, el ingeniero de *software* Jacky Alciné señaló que los algoritmos de reconocimiento de imágenes de Google Photos clasificaban a sus amigos afrodescendientes como "gorilas"[3]. En su momento, la compañía Google se disculpó con Alciné y se comprometió a solucionar el algoritmo. Sin embargo, un nuevo informe de Wired en el 2018 identificó que la compañía simplemente ha bloqueado sus algoritmos de reconocimiento de imágenes para que no identifiquen a los gorilas —por completo—; presumiblemente, prefiere limitar el servicio en lugar de arriesgarse a otra categorización errónea[4].

A su vez, en el 2012, Target alcanzó un nuevo nivel de seguimiento de clientes con la ayuda del uso combinado de datos de consumo. El estadista Andrew Pole identificó veinticinco productos que, cuando se compran juntos, indican que una mujer probablemente está embarazada. El valor de esta información consistía en que Target podía enviar cupones a la mujer embarazada en un periodo costoso y adictivo de su vida[5].

De esta forma, diversas compañías en diferentes sectores recolectan información sobre los usuarios y su comportamiento en línea para crear un determinado perfil que almacena sus gustos, intereses, hábitos de compra y grupos sociales a los que pertenece[6]. Se puede afirmar,

[2] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It", *The New York Times*, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[3] Tom Simonite, "When It Comes to Gorillas, Google Photos Remains Blind" *Wired*, 2018, https://www.wired.com/story/when-it-comes-to-gorillas-google-photos-remains-blind/.

[4] *Ibid*. Megan Garcia, "Racist in the Machine: The Disturbing Implications of Algorithmic Bias", *World Policy Journal* 33, n.º 4 (2016): 111-117, https://muse.jhu.edu/article/645268/summary.

[5] Fernando Duarte, "5 algoritmos que ya están tomando decisiones sobre tu vida y que quizás tú no sabías", *BBC News Mundo*, 2018, https://www.bbc.com/mundo/noticias-42916502; Charles Duhigg, "How Companies Learn Your Secrets", *The New York Times*, 2012, https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[6] Monique Mann y Tobias Matzner, "Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-Discrimination in Responding to Emergent Discrimination", *Big Data & Society* 6, n.º 2 (16 de julio, 2019), https://doi.org/10.1177/2053951719895805.

entonces, que la determinación de perfiles en línea constituye una versión más sofisticada, eficiente y poderosa de los antiguos estudios tradicionales de segmentación demográfica hechos por las investigaciones de mercadeo. Así, la información reunida sobre los usuarios de internet se almacena en grandes bases de datos, que se organizan de tal manera que, con ayuda de los *softwares* de IA, pueden crear correlaciones sobre el comportamiento e intereses del usuario.

Los anteriores casos son solo un abrebocas de las implicaciones jurídicas y éticas del uso de la IA para la determinación del perfil web (Clear View AI, 2019), la determinación de un grupo social (Google Photos, 2015), así como la determinación en las decisiones de consumo (Target, 2012). Estas prácticas han sido objeto de un intenso escrutinio de diversos analistas y académicos, debido a las implicaciones en materia de privacidad, derechos digitales y posibles casos de discriminación. Así, como resultado de estas prácticas diversos gobiernos han empezado a discutir los limites que estas tecnologías deberán tener desde su diseño hasta su implementación[7].

Actualmente, el uso de algoritmos sofisticados que analizan grandes cantidades de datos del consumidor, por ejemplo, permite a los diversos proveedores de bienes y servicios perfilar sus productos a un determinado nicho de consumidores[8]. En este sentido, expertos afirman que la próxima generación de comercio electrónico reduce en un amplio margen la libertad del consumidor y pone en el centro del debate a los agentes digitales basados en algoritmos, que pueden manejar transacciones enteras: usar datos para predecir las preferencias de los consumidores, elegir los productos o servicios por comprar, negociar e incluso

[7] High Level Independent Group on Artificial Intelligence (AI HLEG), "Ethics Guidelines for Trustworthy AI", *European Commission*, 2019.

[8] Steven M. Shugan, "The Cost of Thinking", *Journal of Consumer Research* 7, n.º 2 (1980): 99-111, https://doi.org/10.2307/2489077; John W. Payne, James R. Bettman y Eric J. Johnson, "Adaptive Strategy Selection in Decision Making", *Journal of Experimental Psychology: Learning, Memory, and Cognition* 14, n.º 3 (1988): 534-552, https://doi.org/10.1037/0278-7393.14.3.534; Joseph Alba *et al*., "Interactive Home Shopping: Consumer, Retailer, and Manufacturer Incentives to Participate in Electronic Marketplaces", *Journal of Marketing* 61, n.º 3 (2 de julio de 1997): 38-53, https://doi.org/10.1177/002224299706100303.

ejecutar la transacción[9]. Así, la toma de decisiones libre e informada podría llegar a transformarse en decisiones automatizadas dependiendo de mi perfil web.

De esta forma, legisladores[10], académicos[11] y defensores de derechos humanos[12] han argumentado que la elaboración de perfiles en línea, así como el uso de *big data* complementado con IA pueden utilizarse para conocer características sensibles de los usuarios, que pueden llegar a determinar factores discriminatorios, tales como las opiniones políticas y religiosas, la orientación sexual o las condiciones médicas de un

[9] Rianne Letschert *et al*., *Feasibility Study to Assess the Possibilities, Opportunities and Needs to Standardise National Legislation on Violence against Women, Violence against Children and Sexual Orientation Violence* (Brussels: European Commission, 2010), https://pure.uvt.nl/portal/files/1371655/Letschert_Identifying_minimum_standards_in_the_field_of_violence_111205_publishers_immediately.pdf; María Lorena Flórez Rojas, "Are Online Consumers Protected from Geo-Blocking Practices within the European Union?", *International Journal of Law and Information Technology* 26, n.º 2 (2018), https://doi.org/10.1093/ijlit/eay004; Jonathan Hill, *Cross-Border Consumer Contracts*, Oxford Private International Law Series (Oxford, Nueva York: Oxford University Press, 2008), https://global.oup.com/academic/product/cross-border-consumer-contracts-9780199276547?cc=it&lang=en&; Minghua He, Nicholas R. Jennings y Ho-Fung Leung, "On Agent-Mediated Electronic Commerce", *IEEE Trans on Knowledge and Data Engineering* 15, n.º 4 (2003): 985-1003.

[10] High Level Independent Group on Artificial Intelligence (AI HLEG), "Ethics Guidelines for Trustworthy AI"; European Commission, "Communication from the Commission to the European Parliament, Artificial Intelligence for Europe" (Bruselas, 2018).

[11] Luciano Floridi, *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality* (Londres: Oxford University Press, 2014), https://www.oii.ox.ac.uk/research/books/the-fourth-revolution/; Sandra Wachter, Brent Mittelstadt y Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *International Data Privacy Law* 7, n.º 2 (2017): 76, http://social.cs.uiuc.edu/papers/pdfs/ICA2014-Sandvig.pdf.

[12] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) y Organización de las Naciones Unidas (ONU), *Declaración sobre la Utilización del Progreso Científico y Tecnológico en Interés de la Paz y en Beneficio de la Humanidad*, 1975, https://www.ohchr.org/SP/ProfessionalInterest/Pages/ScientificAndTechnologicalProgress.aspx; Iris Benohr, *EU Consumer Law and Human Rights*, Oxford Studies in European Law (Oxford, Nueva York: Oxford University Press, 2014), https://global.oup.com/academic/product/eu-consumer-law-and-human-rights-9780199651979?cc=us&lang=en&; Council of Europe, "Human Rights Guidelines for Internet Service Providers" (Council of Europe, 2008).

usuario; información que puede venderse y compartirse en un mundo interconectado. Sobre el particular, algunos autores[13] argumentan incluso que el término *discriminación* trasciende a un ámbito económico, como el de discriminación de precios en línea para referirse a determinadas prácticas que se basan en la recopilación y análisis de datos sobre consumidores actuales o potenciales, para definir un precio para ellos en específico, diferenciando entre clientes o grupos de clientes, con fines de adaptación de precios, basados en diversas características sensibles observadas o inferidas de esos clientes[14].

Las diferentes situaciones que han sucedido y seguirán sucediendo hacen eco sobre la necesidad de afrontar institucionalmente los impactos de estas tecnologías disruptivas, con el fin de proteger a todos los actores que interactúen con ellas. Desde el desarrollador hasta el usuario final tienen un conglomerado de derechos y deberes frente a la IA y otras tecnologías; incluso, este mismo sistema debe desenvolverse bajo los parámetros de la ética y la moral[15]. Así, en palabras de Mark Coeckelbergh "[d]ado que los sistemas de IA ya se usan hoy en día, estas preocupaciones no solo son filosóficamente interesantes, sino que también son muy prácticas y urgentes"[16].

De esta forma, la interacción entre el potencial, la necesidad digital moderna y lo desconocido de la IA dan paso a interrogantes sobre los riesgos

[13] Richard Steppe, "Online Price Discrimination and Personal Data: A General Data Protection Regulation Perspective", *Computer Law and Security Review* 33, n.º 6 (1.º de diciembre del 2017): 768-785, https://doi.org/10.1016/j.clsr.2017.05.008; Frederik Zuiderveen Borgesius y Joost Poort, "Online Price Discrimination and *EU* Data Privacy Law", *Journal of Consumer Policy* 40, n.º 3 (2017): 347-366, https://doi.org/10.1007/s10603-017-9354-z.

[14] Siva Viswanathan *et al*., "Online Infomediaries and Price Discrimination: Evidence from the Automotive Retailing Sector", *Journal of Marketing* 71, n.º 3 (2 de julio del 2007): 89-107, https://doi.org/10.1509/jmkg.71.3.089; Michael R. Baye, John Morgan y Patrick Scholten, "The Value of Information in an Online Consumer Electronics Market", *Journal of Public Policy and Marketing* 22, n.º 1 (2003): 17-25, https://doi.org/10.1509/jppm.22.1.17.17625.

[15] Aníbal Monasterio Astobiza, "Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos", *Dilemata* 9, n.º 24 (2017): 185-217, https://doi.org/1989-7022.

[16] Mark Coeckelbergh, "Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability", *Science and Engineering Ethics*, n.º 26 (24 de octubre del 2019): 1-18, https://doi.org/10.1007/s11948-019-00146-8.

jurídicos y éticos que esta tecnología presenta. El problema jurídico que se busca responder en este capítulo es si la actual regulación en materia de protección de datos y del consumidor son suficientes para afrontar el fenómeno del determinismo algorítmico en Colombia, el cual estipula los potenciales hábitos, gustos y grupos a los que los usuarios deben pertenecer.

Para dar respuesta a esta pregunta de investigación, primero se describe el contexto tecnológico de la noción general de IA y cómo esta tecnología ha impactado en la creación de perfiles web. A continuación, se describe el concepto de determinismo algorítmico y cómo influye en las decisiones automatizadas de los usuarios de internet. Luego, se analiza el régimen de protección de datos colombiano con relación a la creación de perfiles web y su posible uso discriminatorio. Enseguida, se analiza el régimen de protección al consumidor para establecer si estas practicas de perfilamiento están reguladas o limitadas en el país. Finalmente, con estos hallazgos, se hacen algunas recomendaciones para que Colombia adopte buenas prácticas en la implementación de IA con base en los riesgos potenciales que presenta. Con ello, se presentan algunas conclusiones finales.

Contexto tecnológico: inteligencia artificial y algoritmos

A diario recibimos noticias sobre el uso de nuevas tecnologías que afectan la forma o el desarrollo estándar de determinada labor. Conceptos como IA, algoritmos, herramientas automatizadas, entre otros, se hacen cada vez más comunes[17]. Esa intromisión tecnológica en el día a día de los consumidores tiene ventajas para una sociedad de consumo, pero a su vez crea un sinnúmero de riesgos para los mismos consumidores. Un concepto que hace unos años parecía un lujo para algunos se ha vuelto una necesidad para todos, y es sin duda el sector de mayor crecimiento y alcance del mundo. La manera de adquirir productos y servicios hoy en día dista mucho de como se hacía en el pasado, no solo por la variedad de productos en el mercado, sino por la agilidad misma para adquirirlos,

[17] Andrea Renda,"Artificial Intelligence Ethics, Governance and Policy Challenges Report of a CEPS Task Force" (Bruselas, 2019), https://www.ceps.eu/wp-content/uploads/2018/03/AI_TFR.pdf.

así como por la infinidad de plataformas para hacerlo. De esta forma, el uso de la IA será una característica determinante de nuestros mercados y sociedades[18]. Los vehículos autónomos, los asistentes a domicilio y los asistentes robóticos en servicios financieros pueden pasar de ser la excepción hoy en día a convertirse en la norma en muy pocos años.

En este sentido, todos los consumidores en la actualidad están rodeados de numerosos dispositivos conectados a internet[19]. En este escenario, las máquinas y los *softwares* inteligentes de aprendizaje automático utilizan la gran cantidad de datos generados por estos dispositivos para tomar decisiones, y en un futuro —no muy lejano— podrán llegar a realizar acciones sin supervisión humana[20]. Todas estas nuevas sinergias entre la tecnología y la vida cotidiana tienen implicaciones importantes sobre la manera en que los consumidores toman decisiones, cómo es la interacción con las empresas privadas y el Gobierno, así como sobre quién será responsable cuando las cosas salgan mal.

Noción de inteligencia artificial y aprendizaje automático

Cómo nace la IA, quién acuñó el término y cómo se usa esta tecnología son interrogantes que continúan desarrollándose, dependiendo del campo de aplicación. A pesar de que el término *inteligencia artificial* fue acuñado en 1956, las raíces del campo se remontan a la década de 1940[21] y la idea de IA se cristalizó en el famoso artículo de Alan Turing en 1950, "Computing Machinery and Intelligence", en el cual se planteó la pregunta: "¿Pueden las máquinas pensar?"[22]. En el documento titulado *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence,* desarrollado por McCarthy *et al*. se considera

[18] World Intellectual Property Organization (WIPO), *WIPO Technology Trends 2019 - Artificial Intelligence* (Suiza, 2019), https://doi.org/978-92-805-3007-0.

[19] *Ibid*.

[20] Big Data Value Association (BDVA), "Data-Driven Artificial Intelligence for European Economic Competitiveness and Societal Progress-Position Statement", 2018.

[21] Warren S. McCulloch y Walter Pitts, "A Logical Calculus of the Ideas Immanent in Nervous Activity", *Bulletin of Mathematical Biophysics* 52, n.º 2 (1990): 99-115.

[22] Alan Turing, "Computing Machinery and Intelligence", *Mind*, n.º 49 (1950).

que "el problema de la inteligencia artificial es hacer que una máquina se comporte de una manera que se llamaría inteligente, tal y como si un humano se comportara de esa forma"[23]. Con todo lo anterior, para efectos de este capítulo, y sin hacer una descripción exhaustiva de la IA, se puede afirmar que las diferentes definiciones pueden enmarcarse en dos dimensiones en relación con el objetivo del análisis. En primer lugar, la dimensión que iguala el desempeño humano, y en segundo lugar la que busca determinar si el objetivo es construir sistemas que razonen o "piensen", o mejor, sistemas que actúen por sí mismos[24].

En cuanto al aprendizaje automático, este es visto como un método por medio del cual se pretende que la máquina pueda aprender por sí misma sin ser programada explícitamente[25]. Se le considera entonces una aplicación de IA que proporciona al sistema la capacidad de aprender y mejorar automáticamente a partir de la experiencia. Dos avances importantes condujeron a la aparición del aprendizaje automático como el catalizador del desarrollo de la IA con la velocidad que tiene actualmente. El primero se dio con el concepto de *comprensión*, acreditado a Arthur Samuel en 1959, según el cual en lugar de enseñarles a las computadoras todo lo que necesitan saber sobre el mundo y cómo llevar a cabo tareas —*programación previa*—, podría enseñárseles a aprender por sí mismas[26]. El segundo avance fue la aparición de internet y el gran aumento en la cantidad de información digital que se genera, almacena y pone a disposición para su análisis[27]. Una vez que se implementaron

[23] John McCarthy *et al*., "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955", *AI Magazine* 27, n.º 4 (15 de diciembre del 2006): 12, https://doi.org/10.1609/AIMAG.V27I4.1904.

[24] Roberto Viola, "Artificial Intelligence, Real Benefits" (Bruselas, 2018), https://ec.europa.eu/digital-single-market/en/news/artificial-intelligence-real-benefits; Yavar Bathaee, "Artificial Intelligence Opinion Liability", *Berkeley Technology Law Journal* 35, n.º 1 (2020): 113, https://doi.org/10.15779/Z38P55DH32.

[25] Judith Hurwitz y Daniel Kirsch, *Machine Learning IBM Limited Edition* (Nueva Jersey: John Wiley & Sons, Inc., 2018), http://www.wiley.com/go/permissions.

[26] Arthur L. Samuel, "Some Studies in Machine Learning Using the Game of Checkers. II-Recent Progress", n. d.; Michal S. Gal, "Algorithmic Challenges to Autonomous Choice", *Mich. Telecomm. & Tech. L. Rev* 25 (2018); Arthur Samuel, "In Memoriam-Arthur Samuel: Pioneer in Machine Learning", *AI Magazine*, n.º 11 (15 de septiembre de 1990), https://doi.org/10.1609/AIMAG.V11I3.840.

[27] Samuel, "Some Studies".

estas innovaciones, se empezó a entrenar las máquinas para que pensaran como seres humanos, y luego conectarlas a internet para darles acceso a toda la información disponible alrededor del mundo digital[28].

Las aplicaciones de aprendizaje automático pueden leer el texto y determinar si la persona que lo escribió está presentando una queja u ofreciendo felicitaciones[29]. También pueden escuchar una pieza musical, decidir si es probable que haga feliz o triste a alguien, y encontrar otras piezas musicales que coincidan con el estado de ánimo. La parte de "aprendizaje" del aprendizaje automático significa que los algoritmos buscan optimizarse a lo largo de una determinada dimensión. Es decir, por lo general intentan minimizar el error o maximizar la probabilidad de que sus predicciones sean verdaderas[30].

De esta forma, el aprendizaje automático se ha convertido en uno de los temas más importantes dentro de organizaciones en el sector privado que buscan diversas maneras de aprovechar los activos de datos para mejorar la visibilidad de sus negocios, así como sus ventas[31]. Debido a que los datos en el ciberespacio son constantemente agregados, los modelos de aprendizaje automático pueden mejorar las soluciones tecnológicas con miras a que estas a su vez estén actualizadas. Así, el aprendizaje automático utiliza una variedad de algoritmos que iterativamente aprenden de los datos —*suministrados o capturados inteligentemente*— para mejorar, describir y predecir resultados[32].

A medida que los algoritmos[33] son alimentados con datos iniciales de entrenamiento, es posible producir modelos más precisos basados en esos datos. Un modelo de aprendizaje automático es el resultado obtenido cuando se entrena un algoritmo de aprendizaje con datos y después del entrenamiento inicial se establece un modelo con una entrada que

[28] BDVA, "Data-Driven Artificial Intelligence"; WIPO, "WIPO Technology Trends 2019".

[29] Judith Hurwitz y Daniel Kirsch, *Machine Learning IBM Limited Edition*.

[30] Quentin André *et al*., "Consumer Choice and Autonomy in the Age of Artificial Intelligence and Big Data", *Customer Needs and Solutions* 5, n.os 1-2 (marzo del 2018): 28-37, https://doi.org/10.1007/s40547-017-0085-8; Gal, "Algorithmic Challenges".

[31] Judith Hurwitz y Daniel Kirsch, *Machine Learning IBM*; Samuel, "Some Studies".

[32] André *et al*., "Consumer Choice and Autonomy"; Gal, "Algorithmic Challenges".

[33] Construcción matemática con una estructura de control finita, abstracta, efectiva y compuesta, dada imperativamente para el logro de un objetivo específico y bajo unas condiciones puntuales.

genera una respuesta de salida, la cual no se ha entregado previamente, pero es el resultado del análisis de esos datos. En otras palabras, un algoritmo predictivo creará un modelo predictivo en la medida en que se proporcionan datos al modelo, el cual arrojará una predicción basada en los datos que entrenaron al modelo. Por ejemplo, cuando visitamos un sitio de comercio electrónico y se empiezan a desplegar productos y servicios que han sido reseñados como: "es probable que se le presenten otros productos similares que le puedan interesar". Estas recomendaciones no están codificadas por un ejército de desarrolladores cada vez que accedemos a un sitio web, por el contrario, se despliegan en el sitio mediante un modelo de aprendizaje automático. El modelo se alimenta con el historial de navegación junto con los datos de compra de otros consumidores "similares" para presentar otros productos análogos que tal vez desee comprar.

En este sentido, la tecnología de IA combinada con diversas técnicas de la ingeniería robótica y de computación perfeccionan cada vez más la imitación del comportamiento humano inteligente[34]. El aprendizaje automático, el análisis del *big data*[35], la computación en la nube[36] y la perfilación algorítmica[37] permiten identificar patrones cada vez más complejos en grandes conjuntos de datos y, en algunos casos, superar en términos de eficiencia a los humanos en ciertas funciones cognitivas[38].

[34] WIPO, "WIPO Technology Trends 2019".

[35] *Big data*: técnica de analítica de datos que contienen una mayor variedad y que se presentan en volúmenes crecientes y a una velocidad superior. El *big data* está formado por conjuntos de datos de mayor tamaño y más complejos, en especial procedentes de nuevas fuentes de datos. Estos conjuntos de datos son tan voluminosos que el *software* de procesamiento de datos convencional sencillamente no puede administrarlos.

[36] La computación en la nube es una tecnología que permite el acceso remoto, desde cualquier lugar del mundo y en cualquier momento, a *softwares*, almacenamiento de archivos y procesamiento de datos por internet, sin la necesidad de conectarse a un ordenador personal o servidor local.

[37] La elaboración de perfiles algorítmicos es una forma de detectar patrones y hacer predicciones a partir de ellos. En la ciencia de la información, la elaboración de perfiles se refiere al proceso de construcción y aplicación de perfiles de usuario generados por el análisis de datos informáticos. Se trata del uso de algoritmos u otras técnicas matemáticas que permiten descubrir patrones o correlaciones en grandes cantidades de datos, agregados en bases de datos.

[38] BDVA, "Data-Driven Artificial Intelligence".

Todo lo anterior reafirma la idea de que la tecnología nos proporciona las herramientas necesarias para mejorar la vida, pero si no se controla, también tiene el poder de discriminar y reforzar los estereotipos y los prejuicios. Así, el avance de los sistemas distribuidos capaces de almacenar y procesar cantidades masivas de datos anteriormente dispares, junto con la aparición de la IA en nuestra vida cotidiana, nos obliga a centrarnos en la forma en que se diseña, prueba, despliega y gobierna, para garantizar que su impacto siga siendo positivo.

Determinismo algorítmico

El determinismo es una doctrina filosófica que sostiene que todo acontecimiento físico, incluyendo el pensamiento y las acciones humanas, está causalmente determinado por la irrompible cadena causa-consecuencia, y, por tanto, el estado actual "determina" en algún sentido el futuro. Existen diferentes formulaciones de determinismo, así, dependiendo del grado se pueden dividir en determinismo débil y fuerte[39]. Mientras que el primero sostiene que es la probabilidad lo que está determinado por los hechos presentes, o que existe una fuerte correlación entre el estado presente y los estados futuros —aun admitiendo la influencia de sucesos esencialmente aleatorios e impredecibles—, el segundo plantea que no existen sucesos genuinamente aleatorios o azarosos, y en general, el futuro es potencialmente predecible a partir del presente[40]. Cabe resaltar que existe una diferencia importante entre la determinación y la predictibilidad de los hechos. La determinación implica exclusivamente la ausencia de azar en la cadena causa-efecto que da lugar a un suceso concreto. La predictibilidad es un hecho potencial derivado de la determinación certera de los sucesos, pero exige que se conozcan las condiciones iniciales (o de cualquier punto) de la cadena de causalidad.

[39] A. C. MacIntyre, "Determinism", *Mind* 66, n.º 261 (1957): 28-41, https://www.jstor.org/stable/2251366; María Milossi, Eugenia Alexandropoulou-Egyptiadou, Konstantinos Psannis, "AI Ethics: Algorithmic Determinism or Self-Determination? The GPDR Approach", *IEEE Internet Computing*, n.º 9 (2021): 1-12, https://doi.org/10.1109.

[40] Slava Polonski, "Algorithmic Determinism and the Limits of Artificial Intelligence", *Oxford Internet Institute Blog*, 2016, https://www.oii.ox.ac.uk/blog/algorithmic-determinism-and-the-limits-of-artificial-intelligence/.

En primer lugar, es relevante mencionar que los algoritmos son un conjunto de instrucciones dadas a un sistema, en forma de *software*, sobre cómo interactuar, manipular y transformar a partir del uso de datos[41]. Así, un algoritmo puede ser tan simple como una técnica para agregar una columna de números o tan complejo como para identificar el rostro de alguien en una imagen. Además, para que sea operativo, debe estar compuesto como un programa que las computadoras puedan entender. Los algoritmos de aprendizaje automático se escriben con mayor frecuencia en uno de varios lenguajes (Java, Python o R.), cada uno de los cuales incluye bibliotecas de aprendizaje automático que admiten y soportan una variedad de algoritmos[42]. Sin embargo, los algoritmos de aprendizaje automático son diferentes de otros algoritmos simples. De esta forma, con la mayoría de los algoritmos, un programador o desarrollador comienza ingresando el valor (*algoritmo*), mientras que con el algoritmo de aprendizaje automático, el proceso es inverso. Así, lo indispensable es ingresar los datos en sí mismos (*bibliotecas de datos*) y estos crearán el modelo. Cuantos más datos se agreguen al algoritmo, este se vuelve más complejo; por tanto, a medida que el algoritmo de aprendizaje automático está expuesto a más y más datos puede crear un algoritmo más preciso[43].

En línea con lo anterior, la omnipresente IA, a pesar de su promesa de ser útil en diversos sectores, plantea numerosos problemas éticos[44]. En diversos sectores, en especial en el del comercio electrónico, los consumidores han identificado que los algoritmos de recomendación son útiles para invertir el tiempo de búsqueda en otras actividades. En este

[41] Hurwitz y Kirsch, *Machine Learning IBM.* Gal, "Algorithmic Challenges", *SSRN Electronic Journal* n.º (24 de mayo del 2017), https://doi.org/10.2139/ssrn.2971456.

[42] Gilles Dowek y Jean-Jacques Lévy, *Introduction to the Theory of Programming* (Londres: Springer-Verlag 2011), https://www.springer.com/gp/book/9780857290755; Monasterio Astobiza, "Ética algorítmica".

[43] Hurwitz y Kirsch, *Machine Learning IBM*; Samuel, "Some Studies".

[44] High Level Independent Group on Artificial Intelligence (AI HLEG), "Ethics Guidelines"; Virginia Dignum, "Ethics in Artificial Intelligence: Introduction to the Special Issue", *Ethics and Information Technology* 20, n.º 1 (1.º de marzo del 2018): 1-3, https://doi.org/10.1007/s10676-018-9450-z; Brent Daniel Mittelstadt *et al*., "The Ethics of Algorithms: Mapping the Debate", *Big Data & Society* 3, n.º 2 (1.º de diciembre del 2016), https://doi.org/10.1177/2053951716679679.

sentido, los usuarios han reconocido los beneficios de contar con este tipo de recomendaciones en su pantalla, sin embargo —en un futuro no tan lejano— podrían manifestarse en sectores como la salud, la seguridad social, los seguros e incluso la agricultura, exacerbando los sesgos y los prejuicios[45]. De allí que se afirme que la noción de determinismo algorítmico hace eco de lo que Winston Churchill dijo una vez sobre los edificios: "We Shape Our Buildings, and Thereafter Our Buildings Shape Us" [Damos forma a nuestros edificios y, a partir de ese momento, nuestros edificios nos dan forma a nosotros], adaptando los edificios a herramientas o algoritmos se puede afirmar que los seres humanos damos forma a nuestros algoritmos; después, ellos nos dan forma a nosotros.

Así, con base en las acciones pasadas de un consumidor, un algoritmo —en su mayoría determinista— puede concluir que a este le gusta comprar productos similares a los comprados por sus amigos cercanos, y, en consecuencia, pueden cambiar los parámetros decisionales del algoritmo. Una amplia variedad de algoritmos hoy en día ya ayuda a los consumidores a tomar decisiones en transacciones de mercado. Algunos, como Kayak, Expedia y Travelocity, ofrecen información sobre precios de vuelos, viajes y estadías. Estas plataformas simplemente recopilan y organizan la información relevante proporcionada por sus propios proveedores (aliados)[46]. Otros, por ejemplo los servicios de calificación tales como TripAdvisor y Yelp[47], ofrecen información sobre la calidad. Sin embargo, algoritmos más sofisticados usan análisis de datos para habilitar la previsión de precios, reducir las opciones y filtrar contenido presentando solo aquellos que se suponen más relevantes, como lo

[45] Mann y Matzner, "Challenging Algorithmic Profiling".

[46] Antonio Maccioni y Riccardo Torlone, "Kayak: A Framework for Just-in-Time Data Preparation in a Data Lake", en *Advanced Information Systems Engineering*, editado por Bo Steinholtz, Arne Sølvberg y Lars Bergman (Springer Verlag, 2018), 474-489, https://doi.org/10.1007/978-3-319-91563-0_29.

[47] Mehrbakhsh Nilashi *et al*., "Travelers Decision Making Using Online Review in Social Network Sites: A Case on TripAdvisor", *Journal of Computational Science* 28 (1.º de septiembre del 2018): 168-179, https://doi.org/10.1016/j.jocs.2018.09.006; Hee Andy Lee, Rob Law y Jamie Murphy, "Helpful Reviewers in TripAdvisor, an Online Travel Community", *Journal of Travel and Tourism Marketing* 28, n.º 7 (octubre del 2011): 675-688, https://doi.org/10.1080/10548408.2011.611739.

hacen los servicios de citas en línea como OKCupid y Tinder[48]. Tales algoritmos se muestran como herramientas para mejorar la elección del consumidor al agregar y organizar datos relevantes para ayudarle a tomar una decisión "informada".

Así, en el contexto de las aplicaciones digitales personalizadas, estas técnicas de aprendizaje estadístico se utilizan para crear una identidad algorítmica para sus usuarios, que abarca varias dimensiones, como los patrones de uso, los gustos, las preferencias, los rasgos de personalidad y la estructura de su gráfico social[49]. Esta identidad digital, sin embargo, no se basa directamente en la personalidad o el sentido del yo de los usuarios, sino en una colección de puntos de datos medibles y en cómo los interpreta la máquina. En otras palabras, la identidad del usuario, por muy compleja que sea, es sustituida por una representación digital imperfecta de sí mismo a los ojos de la IA.

El ritmo del progreso de la IA conlleva retos, tales como los sesgos de los algoritmos que pueden amplificar nuestros propios sesgos y profundizar las divisiones sociales. Así, las aplicaciones de IA utilizan datos de nuestras acciones pasadas para anticipar nuestras necesidades en el futuro, lo cual termina siendo más problemático, porque tiende a reproducir patrones de comportamiento establecidos, proporcionando viejas respuestas a nuevas preguntas; el llamado *determinismo algorítmico*. Esto resulta peligroso porque excluye nuestra necesidad de experimentación y exploración, a la vez que ignora la multiplicidad de nuestra identidad. Con ello, la IA solo puede emplear en sus cálculos los datos trazados históricamente, que luego se utilizan para anticipar las necesidades de los usuarios y hacer predicciones sobre el futuro. Un ejemplo de ello fue el uso de redes neuronales entrenadas con imágenes de anteriores presidentes estadounidenses que predijo que Donald Trump

[48] Cédric Courtois y Elisabeth Timmermans, "Cracking the Tinder Code: An Experience Sampling Approach to the Dynamics and Impact of Platform Governing Algorithms", *Journal of Computer-Mediated Communication* 23, n.º 1 (1.º de enero del 2018): 1-16, https://doi.org/10.1093/jcmc/zmx001.

[49] Estee N. Beck, "The Invisible Digital Identity: Assemblages in Digital Networks", *Computers and Composition* 35 (1.º de marzo del 2015): 125-140, https://doi.org/10.1016/J.COMPCOM.2015.01.005; Milton L. Mueller et al., "Digital Identity: How Users Value the Attributes of Online Identifiers", *Information Economics and Policy* 18, n.º 4 (1.º de noviembre del 2006): 405-422, https://doi.org/10.1016/J.INFOECOPOL.2006.04.002.

ganaría las elecciones presidenciales, después de haber sido entrenadas con imágenes de expresidentes (hombres). Como no había presidentas de Estados Unidos en el conjunto de datos, la IA no pudo deducir que el género no era una característica relevante para el modelo[50]. A partir del anterior ejemplo, se puede afirmar que las inferencias que la IA realiza de un conjunto de datos pueden dar lugar a sistemas de recomendación cada vez más deterministas, que tienden a reforzar las creencias y prácticas existentes, similares a las cámaras de eco de nuestras redes sociales.

A manera de conclusión preliminar, el determinismo algorítmico hace referencia a un algoritmo que, en términos informales, es completamente predictivo si se conocen sus datos de entrada, y de esta forma, siempre producirá la misma salida, toda vez que la máquina interna pasará por la misma secuencia de estados. Piénsese, por ejemplo, en el entrenamiento de asistentes virtuales o robóticos en hospitales o centros de cuidado de adultos mayores en donde las funciones de estos asistentes sea levantar pacientes, vigilar su bienestar, interconectarlos con la unidad sanitaria y su médico, informar sobre el estado de salud a la farmacia más cercana y solicitar medicamentos si es necesario[51]. En este caso, si se entrena al asistente virtual o robótico con la información sobre estas labores, *en teoría* obtendremos el mismo resultado, ¿verdad? Pero, ¿qué ocurre si un sistema de IA recomienda un medicamento equivocado para un paciente o no detecta un tumor en una exploración radiológica?

Estos son los riesgos a los que nos enfrentamos cuanto más dependamos de los algoritmos personalizados en la vida cotidiana, pues estos se encargan de moldear lo que vemos, lo que leemos, con quién hablamos y cómo vivimos. Al centrarse implacablemente en el *statu quo*, las nuevas recomendaciones sobre libros para leer, películas para ver y personas para conocer nos darán más de las mismas cosas que nos han encantado anteriormente. En esto consiste el determinismo algorítmico.

[50] Li Mu, "Russian Neural Networks Predict Donald Trump Will Be Next US President", en *ImageNet Large Scale Visual Recognition Challenge 2016 (ILSVRC2016)*, 2016, https://www.ewdn.com/2016/08/08/neural-networks-see-donald-trump-as-us-president/.

[51] Mateus de Oliveira Fornasier, "The Applicability of the Internet of Things (IOT) Between Fundamental Rights to Health and to Privacy", *Revista de Investigações Constitucionais* 6, n.º 2 (31 de enero del 2020): 297-321, https://doi.org/10.5380/RINC.V6I2.67592.

Así, los conceptos de IA, aprendizaje automático, *big data* y determinismo algorítmico no podrían considerarse sinónimos, sino complementarios, dependiendo del campo de aplicación. Por un lado, la IA es una rama de la informática que se ocupa de la simulación del comportamiento inteligente en las computadoras[52]. Es decir, la capacidad de una máquina para imitar el comportamiento humano, como la percepción visual, el reconocimiento de voz, la toma de decisiones y la traducción entre idiomas. Existen diversos métodos para simular la inteligencia humana, que usan o no sistemas de aprendizaje automático o simplemente una base de datos con posibilidades de respuesta (árboles de decisiones)[53]. Con todo lo anterior, se plantean diversas implicaciones en materia de derechos del consumidor y protección de datos.

Desventajas y riesgos del determinismo algorítmico

Desde la investigación científica hasta el diagnóstico médico, y desde la ingeniería de precisión hasta la cirugía, las decisiones automatizadas y la IA podrían generar beneficios prometedores en la forma en que se realizan diversas actividades. Las tecnologías de IA están siendo cada vez más utilizadas por las comunidades de investigación científica y médica para progresar más rápido e innovar mejor en muchas áreas. Así, gracias al análisis de *big data*, el océano de datos recopilados por las empresas se puede utilizar para personalizar los servicios y el contenido de una manera que antes no era posible.

Lo anterior replantea conceptos tradicionales del derecho de consumo sobre cómo operan los mercados y si seguirá teniendo sentido hablar acerca de la elección libre del consumidor, así como autodeterminación informativa, cuando las preferencias se definen, predicen y configuran mediante algoritmos deterministas. En este sentido, los legisladores y juristas deben reevaluar sus herramientas para lidiar efectivamente con

[52] Viola, "Artificial Intelligence, Real Benefits"; WIPO, "WIPO Technology Trends 2019"; European Commission, "Communication from the Commission".

[53] European Commission, "Inteligencia artificial: Un enfoque europeo orientado a la excelencia y la confianza" (Bruselas, 2020), https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_es.pdf; High Level Independent Group on Artificial Intelligence (AI HLEG), "Ethics Guidelines".

fallas regulatorias y de mercado que pueden surgir en este ecosistema digital. Así, teniendo en cuenta que los algoritmos se encuentran a diario, estos pueden generar daños y riesgos, tales como: (1) limitar la elección y autonomía del consumidor; (2) aumentar las vulnerabilidades de los consumidores a decisiones ineficientes tomadas en su nombre; (3) ocasionar daños de seguridad; y (4) crear riesgos en el entorno psicológico y social[54].

En este sentido, la aplicación de estas técnicas conlleva desafíos tanto para los consumidores como para los reguladores y proveedores en diversas áreas, como la protección de derechos digitales, la protección de datos, la responsabilidad algorítmica y la auditoría de las decisiones automatizadas. Sin embargo, para efectos de este capítulo se analizan de forma general tres riesgos más prominentes en relación con el consumidor, el mercado y la sociedad en general, los cuales son la base para el análisis sobre las decisiones automatizadas por algoritmos deterministas.

Patrones oscuros y ausencia de transparencia

Cada vez que los consumidores interactúan con tecnologías que funcionan gracias a la intervención de la IA, se enfrentan a una ola de contenido personalizado y dirigido "especialmente para un consumidor", a menudo sin siquiera saberlo. Los perfiles de usuario y los algoritmos son invisibles para los consumidores, que por lo general no pueden optar por no participar de esta decisión de perfilamiento. De esta forma el análisis de *big data* permite a las compañías estudiar el patrón de comportamiento de los usuarios y predecir las respuestas emocionales necesarias para hacer que el usuario actúe y encontrar qué estímulos pueden usarse para provocar tales respuestas[55]. Así, *los consumidores no tienen forma de conocer los perfiles que se acumulan sobre ellos ni la información sobre el método subyacente utilizado para identificarlos*.

[54] Anne Britt Gran, Peter Booth y Taina Bucher, "To Be or Not to Be Algorithm Aware: A Question of a New Digital Divide?", *Information Communication and Society* 1790, n.º 24 (2020): 12, https://doi.org/10.1080/1369118X.2020.1736124; Courtois y Timmermans, "Cracking the Tinder Code".

[55] Klaus Wertenbroch *et al*., "Autonomy in Consumer Choice", *Mark Lett*, n.º 31, 429-439 (2020), acceso, 1.º de julio del 2021, https://doi.org/10.1007/s11002-020-09521-z.

Con base en lo anterior se han identificado dos problemas complementarios. El primero, en los sistemas de IA, denominado la *caja negra*[56]. Este problema consiste en que el propio sistema no tiene claridad de cómo exactamente llega a su decisión final[57]. Esta falta de transparencia en el proceso hace que incluso los desarrolladores desconozcan la forma en que la IA llega a una decisión en particular[58]. En otras palabras, no se sabe lo que están haciendo cuando usan este tipo de IA para decidir o actuar por ellos, por lo que se configura la ignorancia del instrumento.

El problema de la caja negra consiste en la imposibilidad de entender el proceso de toma de decisiones de una IA basada en *deep learning*. Una red neuronal profunda usualmente cuenta con inmensas cantidades de capas neuronales, que se relacionan entre sí, y que fueron construidas con millones de datos; es común que se vuelva imposible identificar cuáles fueron los patrones que siguió una IA en el momento de solucionar un problema[59]. En otras palabras, una IA basada en *deep learning* va a solucionar el problema con base en tantas subreglas generales interconectadas, que no será posible identificar cuáles fueron las neuronas, o capas de neuronas, que determinaron una solución en un caso concreto. Así, aunque el *deep learning* incrementa la capacidad de cualquier IA, también eleva su "opacidad", pues si bien es posible conocer los datos con que una de estas IA fue entrenada, y las distintas capas que fueron desarrolladas, la cantidad de parámetros que puede procesar al mismo

[56] Sandra Wachter, Brent Mittelstadt y Chris Russell, "Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR", *Harvard Journal of Law & Technology* 31, n.º 2 (6 de octubre del 2018), https://doi.org/10.2139/SSRN.3063289

[57] Coeckelbergh, "Artificial Intelligence, Responsibility"; Floridi, *The Fourth Revolution*.

[58] María Lorena Flórez Rojas y Juliana Vargas Leal, "El impacto de las herramientas de inteligencia artificial: Un análisis en el sector público en Colombia", en Carolina Aguerre *et al*., *Inteligencia artificial en América Latina y el Caribe: Ética, gobernanza y políticas*, 2020, https://guia.ai/wp-content/uploads/2020/05/GECTI-El-impacto-de-herramientas-de-inteligencia-artificial.pdf.

[59] Chris McNicholas, Derek Bell y Julie Reed, "Opening the 'black box' of plan-do-study-act cycles: Achieving a scientific yet pragmatic approach to improving patient care", *BMJ Quality & Safety* 23, n.º 4 (1.º de abril del 2014): 352, https://doi.org/10.1136/bmjqs-2014-002893.11; John Zerilli *et al*., "Algorithmic Decision-Making", *Minds and Machines,* n.º 29 (2019): 555-578, https://doi.org/10.1007/s11023-019-09513-7.

tiempo, debido al inmenso número de capas que se relacionan entre sí, no permitirá determinar cómo la IA tomó la decisión[60].

El segundo problema es el de los *patrones oscuros* (*dark patterns* en inglés), que se caracterizan por ser elementos de diseño en la interfaz del sitio web que eluden la autonomía del consumidor[61]. Estos patrones, a diferencia de los algoritmos de caja negra, son elementos de diseño que pueden incrustarse por medio de los botones que pulsamos y el texto por el que navegamos. Aunque se pueden ver, también pueden estar discretamente camuflados. De esta forma, en diversos sitios web existen patrones oscuros para que una organización reúna algo de valor para el usuario. Ese valor que se intercambia es algo a lo que el usuario probablemente no habría renunciado si pudiera ejercer su autonomía y elegir lo que quiere revelar o comprar[62].

Sin embargo, los patrones oscuros no son nuevos. Los diseños engañosos han existido tanto en las interfaces analógicas como en las digitales. Los patrones oscuros son interfaces de usuario que benefician a un servicio en línea al inducir a los usuarios a tomar decisiones que de otro modo no harían. Algunos patrones oscuros engañan a los usuarios, mientras que otros los manipulan o coaccionan de forma encubierta para que tomen decisiones que no les convienen. A manera de ejemplo, TurboTax ocultó en su página su programa de declaración de impuestos gratuita para usuarios con bajos ingresos, exigido por el Gobierno de Estados Unidos, con el fin de que utilizaran su programa pago[63]. Así, muchos patrones oscuros se han adoptado a gran escala en la web y se han catalogado docenas de patrones, como el de fastidiar al usuario, obstruir el flujo de una tarea y establecer valores predeterminados intrusivos para la privacidad. Sobre el particular, Harry Brignull y otros

[60] André *et al*., "Consumer Choice and Autonomy".

[61] Arvind Narayanan *et al*., "Dark Patterns: Past, Present, and Future The Evolution of Tricky User Interfaces", *Communications of the ACM* 63, n.º 9 (2020): 3, https://doi.org/10.1145/3397884.

[62] Colin M. Gray *et al*., "The Dark (Patterns) Side of UX Design", en *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Nueva York: ACM, 2018), https://doi.org/10.1145/3173574.3174108.

[63] L. Elliott, J., Waldron, "Here's How TurboTax Just Tricked You Into Paying to File Your Taxes-ProPublica", 2019, https://www.propublica.org/article/turbotax-just-tricked-you-into-paying-to-file-your-taxes.

investigadores han encontrado patrones oscuros en más de 1200 sitios de comercio electrónico, lo cual demuestra que aproximadamente 95 % de las aplicaciones de Android contienen patrones oscuros, que tienen la potencialidad de manipular el comportamiento del usuario[64]. A pesar de que el concepto de patrones oscuros ha irrumpido recientemente, estos son el resultado de tres tendencias de hace décadas: (1) las prácticas engañosas, (2) las interferencias en política pública, y (3) la comunidad del diseño[65]. En esta línea, algoritmos que utilizan un sistema de caja negra o de patrones oscuros no están expuestos al escrutinio público y carecen de transparencia precisamente porque el mismo sistema está diseñado de esa forma.

Como punto de inflexión adicional, los algoritmos usados, por lo general, están protegidos por derechos de propiedad intelectual y secretos industriales, lo que desemboca en un secretismo y una ausencia de transparencia frente al uso de esta tecnología[66]. Debido a la falta de transparencia, los usuarios no saben cómo se han analizado sus datos personales, con qué fin y por quién, o por qué recibieron un contenido o respuesta específicos. Toda vez que, en la mayoría de los casos, los consumidores mostrarán un patrón de conducta similar a lo visto en relación con los contratos en línea: aceptar el algoritmo, tomar una elección por defecto sin profundizar en los detalles, ni comprobar si se hizo una elección óptima. Así, es probable que sea difícil solucionar este tipo de fallas en el algoritmo, que involucran incógnitas desconocidas, y a su vez se delega una responsabilidad innecesaria en cabeza del consumidor: la supervisión de estos algoritmos sofisticados y opacos.

[64] Arunesh Mathur *et al*., "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites", *Proceedings of the ACM on Human-Computer Interaction* (1.º de noviembre del 2019), https://doi.org/10.1145/3359183.

[65] *Ibid*.

[66] Mariateresa Maggiolino, "EU Trade Secrets Law and Algorithmic Transparency", *Bocconi Legal Studies Research*, n.º 27 (22 de abril del 2019), https://doi.org/10.2139/ssrn.3363178; Simone Natale y Andrea Ballatore, "Imagining the Thinking Machine: Technological Myths and the Rise of Artificial Intelligence", *Convergence* 26, n.º 1 (1.º de febrero del 2020): 3-18, https://doi.org/10.1177/1354856517715164; Solon Barocas, Sophie Hood y Malte Ziewitz, "Governing Algorithms: A Provocation Piece", *Pat. & Trademark Off. Soc'y*, n.º 69 (10 de abril de 1987), https://doi.org/10.2139/ssrn.2245322.

Discriminación: decisiones automatizadas que sesgan

En este entorno de manipulación de preferencias y elecciones (in)conscientes, los consumidores son altamente vulnerables a ser manipulados por las empresas en una elección específica de compra. Esto puede conducir a daños económicos y sociales, cuando, por ejemplo, se niega un crédito o un seguro al consumidor en función de elementos irrelevantes y claramente discriminatorios, como el género, la raza, la religión, la dirección postal o su geolocalización[67]. Así, los algoritmos pueden acelerar la desigualdad económica y política, en especial en un país como Colombia, con una diversidad cultural y social tan alta.

Los consumidores, según su perfil previamente establecido por el algoritmo, se asignan a segmentos de mercado con un grado creciente de precisión. Esta categorización puede resultar problemática en varias situaciones que pueden ocasionar un tipo de discriminación. Por un lado, se puede realizar una segmentación errónea, por sesgos en las bases de datos o en los datos mismos[68]. En este sentido, el problema ocurre en la fase inicial de la creación de perfiles, toda vez que esta ha alcanzado un resultado incorrecto y en consecuencia unas recomendaciones incorrectas. Esto podría deberse a errores inherentes en la técnica informática del análisis estadístico o a bases de datos sesgadas que pueden hacer que el sistema llegue a falsos positivos o falsos negativos[69]. Así, la discriminación puede ocurrir cuando la entrada de datos sobre el consumidor no es lo suficientemente relevante como para llegar a una conclusión correcta y las consecuencias de tales decisiones automatizadas pueden ser graves,

[67] Flórez Rojas, "Are Online Consumers Protected…?"; Dagmar Schiek y Victoria Chege, *European Union Non-Discrimination Law: Comparative Perspectives on Multidimensional Equality Law* (Routledge, 2009), https://books.google.de/books?id=y5np7xd90ioC; Marketa Trimble, "Geoblocking and 'Legitimate Trade'", en *Intellectual Property and Obstacles to Legitimate Trade*, editado por Heath Christopher, Anselm Kamperman y Anke Moerland (US: Wolters Kluwer, 2018), https://papers.ssrn.com/abstract=3135036.

[68] Flórez Rojas, "Are Online Consumers Protected…?"; Timothy J. Richards, Jura Liaukonyte y Nadia A. Streletskaya, "Personalized Pricing and Price Fairness", *International Journal of Industrial Organization* 44 (1.º de enero del 2016): 138-153, https://doi.org/10.1016/j.ijindorg.2015.11.004.

[69] Gal, "Algorithmic Challenges"; Flórez Rojas, "Are Online Consumers Protected…?".

como, por ejemplo, el usuario puede verse privado de un servicio o se le puede negar el acceso a la información[70].

A manera de ejemplo, diversos grupos de investigación y auditoría han centrado sus investigaciones en Watson para Oncología de IBM para proyectos relacionados con pacientes con cáncer. Una auditoría realizada en el 2016 por la Universidad de Texas descubrió que el centro oncológico MD Anderson Cancer Center gastó sesenta y dos millones de dólares en el proyecto antes de cancelarlo. En principio, el sistema Watson aprendería ingiriendo la vasta literatura médica sobre el cáncer y los registros de salud de pacientes reales con esta enfermedad, a fin de examinar cientos de variables en estos registros —incluyendo datos demográficos, características del tumor, tratamientos y resultados—, para que así encontrara patrones invisibles para los humanos. A pesar de que Watson aprendió con bastante rapidez a escanear artículos sobre estudios clínicos y a determinar los resultados básicos, resultó imposible enseñarle a leer los artículos como lo haría un médico, tampoco pudo analizar un tratamiento nuevo y aplicarlo pues los datos históricos no eran suficientes.

En el 2018, por ejemplo, la FDA aprobó un nuevo fármaco contra el cáncer "agnóstico para los tejidos" que es eficaz contra todos los tumores que presentan una mutación genética específica. El fármaco se aprobó por la vía rápida con base en resultados en solo cincuenta y cinco pacientes, de los cuales cuatro tenían cáncer de pulmón. Sin embargo, Watson no cambiará sus conclusiones basándose en solo cuatro pacientes (datos históricos)[71].

Por otro lado, también es posible que se llegue a discriminar si quienes controlan los algoritmos intentan intencionalmente lograr resultados injustos, discriminatorios o sesgados para excluir a ciertos grupos

[70] Trimble, "Geoblocking and 'Legitimate Trade'"; Flórez Rojas, "Are Online Consumers Protected…?".

[71] Eliza Strickland, "IBM Watson, Heal Thyself: How IBM Overpromised and Underdelivered on AI Health Care", *IEEE Spectrum* 56, n.º 4 (1.º de abril del 2019): 24-31, https://doi.org/10.1109/MSPEC.2019.8678513; Xavier Frank, "Is Watson for Oncology per se Unreasonably Dangerous?: Making A Case for How to Prove Products Liability Based on a Flawed Artificial Intelligence Design", *American Journal of Law & Medicine* 45, n.os 2-3 (1.º de mayo del 2019): 273-294, https://doi.org/10.1177/0098858819871109.

de personas[72]. En este sentido, nos encontramos en la segunda fase del algoritmo de recomendación, en donde mediante esa elaboración de perfiles se indica que es muy probable que un individuo pertenezca a un determinado grupo de la sociedad y, por lo tanto, no se proporciona una invitación para comprar un servicio, o las ofertas de ese individuo se rechazan automáticamente. Sobre este punto, es importante recalcar que puede darse un tipo de discriminación de forma individual al usuario, pero a su vez a un grupo de usuarios que en términos del algoritmo son similares[73].

Para ilustrar mejor estas conductas discriminativas, se puede recordar el primer episodio de la tercera temporada de la serie de Netflix, *Black Mirror*, que evidencia cómo el uso constante de estas nuevas tecnologías hará al usuario tecnodependiente de los algoritmos de clasificación en aras de "encajar" o ser perfilado en determinado grupo social según el impacto de las redes sociales[74]. En el episodio denominado *Nosedive*, con una única plataforma de medios sociales permiten a los usuarios calificar todas sus interacciones en línea y en persona en una escala de cinco estrellas. Así, todos los ciudadanos desplegaban en su frente ese puntaje "social", que determinaba su valor en la sociedad, su acceso a los servicios y su empleabilidad[75]. Este capítulo resume cómo el algoritmo

[72] Verbraucherzentrale, *Geo-Blocking-Tearing down Borders for Digital Content* (Germany: The Federation of German Consumer Organisations, 2017), https://www.vzbv.de/sites/default/files/2017_vzbv_factsheet_geo-blocking_digital_content_1.pdf; Flórez Rojas, "Are Online Consumers Protected…?".

[73] Christian A. Meissner y John C. Brigham, "Thirty Years of Investigating the Own-Race Bias in Memory for Faces: A Meta-Analytic Review", *Psychology, Public Policy, and Law* 7, n.º 1 (2001): 3-35, https://doi.org/10.1037/1076-8971.7.1.3; George E. Schreer, Saundra Smith y Kirsten Thomas, "'Shopping While Black': Examining Racial Discrimination in a Retail Setting", *Journal of Applied Social Psychology* 39, n.º 6 (1.º de junio del 2009): 1432-1444, https://doi.org/10.1111/j.1559-1816.2009.00489.x.

[74] Tasha Robinson, "Black Mirror's Third Season Opens with a Vicious Take on Social Media", *The Verge*, 2016, https://www.theverge.com/2016/10/24/13379204/black-mirror-season-3-episode-1-nosedive-recap.

[75] M. Angela Cirucci y Barry Vacker, *Black Mirror and Critical Media Theory* (Rowman & Littlefield, 2018), https://books.google.com.co/books?hl=en&lr=&id=UkNsDwAAQBAJ&oi=fnd&pg=PR5&dq=black+mirror+implications+in+social+life&ots=QnNWlYHb8e&sig=6xY5JxiHOAgqEHN-JeTSEH83z-8&redir_esc=y#v=onepage&q=black mirror implications in social life&f=false; Chiara Modugno y Tonny Krijnen, "Through the *Black Mirror*: Discourses on Gender and Technology

califica a cada ciudadano y determina a qué puede acceder y a qué no en términos sociales, culturales y de educación.

No obstante, hoy en día no estamos tan alejados de esta clasificación algorítmica en diferentes aspectos de nuestra vida. Así, en China ya se ha evidenciado el primer intento de clasificación social por medio de puntajes con la plataforma Zhima Credit, una calificación de "crédito personal" asociada con Alipay, la principal forma de pago móvil en China. En este esquema, los usuarios reciben un puntaje entre 350 (bajo) y 950 (alto), y se premia a aquellos que tengan "buenos" puntajes con beneficios y recompensas[76]. De esta forma, determinadas actitudes del usuario, como pagar las deudas, le darán una buena calificación, pero también tendrán ciertas calificaciones los productos que elige comprar y, lo que es más importante, la compañía que mantiene. De los anteriores ejemplos, se puede inferir que el uso de esta tecnología para segmentar a los usuarios más allá de unas meras recomendaciones de compra en línea puede tener repercusiones en acceso a servicios de salud o de cultura.

De esta forma, este tipo de categorización en el mercado puede conducir a un tratamiento diferente según el usuario —*discriminación indirecta*—. Los individuos reciben diferentes tipos de precios o de ofertas y promociones especiales porque están asociados con un determinado grupo, mientras que otros no tienen acceso a las mismas ofertas[77]. Sumado a lo anterior, debe tenerse en cuenta que los registros digitales del comportamiento del consumidor pueden revelar datos altamente sensibles, no solo en términos de preferencias, sino también en relación con la orientación sexual, la edad, el género y las opiniones religiosas y políticas. A manera de ejemplo, las personas que el algoritmo ha clasificado

---

in Popular Culture", *Catalan Journal of Communication & Cultural Studies* 12, n.º 1 (19 de mayo del 2020): 3-19, https://doi.org/10.1386/cjcs_00011_1; Robinson, "Black Mirror's Third Season".

[76] Alice Vincent, "Black Mirror Is Coming True in China, Where Your 'rating' Affects Your Home, Transport and Social Circle", *The Telegraph*, 2017, https://www.telegraph.co.uk/on-demand/2017/12/15/black-mirror-coming-true-china-rating-affects-home-transport/.

[77] John G. Lynch y Dan Ariely, "Competition on Price, Quality, and Distribution", *Marketing Science* 19, n.º 1 (2000): 83-103, www.bizrate.com; Borgesius and Poort, "Online Price Discrimination".

como adineradas pueden recibir anuncios sobre un tratamiento médico innovador solo porque se considera que pueden pagarlo, mientras que otros usuarios pueden ser excluidos de estos servicios por pertenecer a un grupo de lo que el algoritmo ha determinado como de "alto riesgo", o con menos capacidad económica, en función de su nacionalidad o sus creencias religiosas[78].

Competencia: decisiones (in)conscientes que afectan el mercado

Cuando los algoritmos se convierten en importantes mediadores del mercado, conectando a proveedores y consumidores con sus creadores u operadores, pueden potencialmente abusar de su poder de mercado para aumentar el gasto de consumidores e incluso afectar las ganancias de los proveedores[79]. En este sentido, los algoritmos y las decisiones que toman por los consumidores, así como las recomendaciones que entregan, pueden llegar a considerarse prácticas comerciales desleales, toda vez que no todos los empresarios pueden competir en las mismas condiciones y existe una significante disparidad entre las grandes empresas tecnológicas y los pequeños empresarios. Además, teniendo en cuenta que el derecho de los mercados tiene una de sus raíces en la idea de que los consumidores deben recibir información esencial para que puedan tomar una decisión informada, será importante preguntarse si la "información esencial" sigue siendo un concepto válido cuando nadie puede volver sobre por qué y cómo se ha tomado una decisión específica, ni siquiera los mismos empresarios.

[78] María Lorena Flórez Rojas, "Legal Uncertainty: Proposed Regulation on Addressing Geo-Blocking", en *Managing Risk in the Digital Society*, coordinado por B. Anglés, *et al.* (Barcelona: Huygens, 2017), 305-319. Adam D. I. Kramer, Jamie E. Guillory y Jeffrey T. Hancock, "Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks", *Proceedings of the National Academy of Sciences of the United States of America* 111, n.º 24 (17 de junio del 2014): 8788-8790, https://doi.org/10.1073/pnas.1320040111.

[79] Hal R. Varian, "Beyond Big Data", *Business Economics* 49, n.º 1 (7 de enero del 2014): 27-31, https://doi.org/10.1057/be.2014.1; BDVA, "Data-Driven Artificial Intelligence".

Actualmente algunos intermediarios digitales con megaplataformas controlan puntos de acceso efectivos para usuarios potenciales, considerándose entonces que existe un alto nivel de concentración en los mercados digitales. Estos incluyen dispositivos inteligentes (iPhone y Kindle), sistemas operativos (iOS y Android), tiendas de aplicaciones (Apple Store y Google Play) y buscadores (Google y Facebook)[80]. El alto nivel de concentración se debe en gran medida a los efectos de red, creados cuando el valor para cada consumidor de usar la plataforma se eleva en paralelo con el número de otros utilizando el sistema[81]. Estos efectos de red se incrementan aún más por el uso del *big data*, al converger el control del contenido, el acceso y los canales de distribución en línea[82]. De esta forma, las grandes plataformas digitales disfrutan inherentemente de las ventajas competitivas en el acceso a un inmenso volumen de información personal de los usuarios.

Es importante destacar que el acceso a tales intermediarios es esencial para la mayoría de los proveedores y distribuidores de productos en el comercio electrónico, ya que generalmente necesitan de ellos para llegar a sus usuarios (por ejemplo, con una tienda de aplicaciones) o para recopilar los datos relevantes (por ejemplo, con un buscador) y así perfilarlos, de tal forma que puedan sugerir recomendaciones de compra[83]. Este proceso de portabilidad de datos entre plataformas es muy común, por ejemplo, cuando un consumidor entra en un determinado sitio web para acceder a comprar un producto (digamos un regalo para dama) y la plataforma le indica diversas opciones para finalizar la compra, entre ellas llenar un formulario de inscripción o inscribirse usando los datos de una plataforma determinada (Facebook o Google). Como resultado, los intermediarios digitales pueden afectar qué algoritmos llegan a usuarios potenciales y en qué términos.

[80] Thulara N. Hewage *et al*., "Review: Big Data Techniques of Google, Amazon, Facebook and Twitter", *Journal of Communications* 13, n.º 2 (1.º de febrero del 2018): 94-100, https://doi.org/10.12720/jcm.13.2.94-100.

[81] Gal, "Algorithmic Challenges".

[82] BDVA, "Data-Driven Artificial Intelligence".

[83] Barocas, Hood y Ziewitz, "Governing Algorithms"; Hewage *et al*., "Review: Big Data"; Varian, "Beyond Big Data".

Implicaciones en la protección de datos personales

El uso de la IA y algoritmos deterministas en el diario vivir de usuarios y consumidores funciona con información filtrada y personalizada. Esta información se recopila a través de todo tipo de canales: redes sociales, fuentes de noticias favoritas del consumidor y las aplicaciones móviles que utiliza. En la etapa de desarrollo, los datos sirven para entrenar los algoritmos y permitirles desarrollar sus capacidades de aprendizaje automático. Una vez en acción, la IA continúa necesitando datos, ya sea simplemente para realizar la tarea para la que ha sido programada y producir una salida, o para continuar aprendiendo y ajustándose en el proceso. En este sencillo escenario, los datos de alimentación del algoritmo, así como los datos generados por este, pueden llegar a considerarse datos personales. El volumen de los datos utilizados, su fuente, la importancia de su precisión, la complejidad de las operaciones de procesamiento de datos y, en algunos casos, la imprevisibilidad y la opacidad del resultado, plantean serios riesgos y desafíos desde el punto de vista de la protección de datos y la privacidad[84].

Uno de estos riesgos asociados puede derivarse del tratamiento inadecuado de datos personales por parte de compañías que muestran un cierto patrón de comportamiento de los consumidores. Por ejemplo, cuando se trata de medidores inteligentes, los algoritmos aprenden lo que está sucediendo en el "hogar inteligente" que luego podría conducir a perfiles de comportamiento, publicidad dirigida y posiblemente también a determinar el comportamiento que podría usarse para evaluar la solvencia del consumidor[85]. Otro riesgo asociado al inadecuado tratamiento de datos personales se resume en el posible daño físico o integridad del consumidor, por ejemplo, en los casos en que los análisis de *big data* utilizan información no contextualizada para influir en el comportamiento del consumidor en cuanto a decisiones relacionadas

[84] Eoghan McKenna, Ian Richardson y Murray Thomson, "Smart Meter Data: Balancing Consumer Privacy Concerns with Legitimate Applications", *Energy Policy* 41 (1.º de febrero del 2012): 807-814, https://doi.org/10.1016/j.enpol.2011.11.049.

[85] P. H. Cheah *et al*., "Consumer Energy Portal and Home Energy Management System for Smart Grid Applications", *10th International Power and Energy Conference, IPEC 2012* (2012), 407-411, https://doi.org/10.1109/ASSCC.2012.6523302.

con la salud, como dejar de fumar[86]. Lo mismo ocurre en el caso de las aplicaciones de *e-health*, que recopilan información sobre los usuarios y combinan contenido de salud y contenido comercial, en última instancia, empujando a los consumidores en una determinada dirección sin que ellos lo sepan.

Los anteriores riesgos determinan que uno de los puntos básicos para implementar IA en diversas áreas sea el desarrollo íntegro de la ley de protección de datos y sus decretos reglamentarios[87]. Sin embargo, hay muchas preguntas relacionadas con el significado, la aplicación práctica y los límites de algunos de los principios fundamentales de la Ley 1581 del 2012, como la transparencia en el procesamiento de datos personales, la minimización de datos, la limitación del propósito y la responsabilidad. Sobre el particular, la Red Iberoamericana de Protección de Datos compiló una guía con el propósito de exponer los principales aspectos jurídicos que involucra el tratamiento de datos personales en los desarrollos de IA, así como de presentar algunas recomendaciones a quienes desarrollan estos productos[88]. Dentro de esta guía, varias de las recomendaciones no solo se enfocan en la verificación de la calidad de los datos recolectados (veracidad), sino también en que se deben efectuar evaluaciones de impacto de privacidad, las cuales deben garantizar la trazabilidad del algoritmo. Así, para efectos de este estudio se analizan a grandes rasgos dos elementos fundamentales que se derivan de la sinergia entre consumidor y titular del dato.

[86] Organisation for Economic Co-operation and Development (OECD), *Artificial Intelligence in Society* (París: OECD, 2019), https://doi.org/10.1787/eedfee77-en; Xiaocheng Li *et al*., "Design of Healthy Eating System Based on Web Data Mining", en *Proceedings-2010 WASE International Conference on Information Engineering*, 346-349, ICIE, 2010, https://doi.org/10.1109/ICIE.2010.89.

[87] Ley Estatutaria 1581 del 2012, 17 de octubre del 2012, por la cual se dictan disposiciones generales para la protección de datos personales. *Diario Oficial* 48587.

[88] Red Iberoamericana de Protección de Datos (RIPD), "Recomendaciones generales para el tratamiento de datos personales en la inteligencia artificial", 2019. https://www.sic.gov.co/sites/default/files/files/pdf/1.

Transparencia y consentimiento en decisiones automatizadas

La IA a menudo implica procesos técnicos muy complejos que son difíciles de explicar y comprender para aquellos que no tienen el conocimiento y la experiencia necesarios para trabajar en el campo. A veces, incluso aquellos involucrados en el desarrollo y uso de la IA pueden tener dificultades para explicar y predecir su funcionamiento y resultados[89]. En este sentido, hablar de conceptos como *consentimiento informado* pierde un tanto el sentido, en la medida en que el consumidor no tendría claro cómo se utilizarán sus datos ni con qué fines. Como ya se explicó, los algoritmos que potencian la IA a menudo operan dentro de "cajas negras" con poca transparencia. Sin embargo, el artículo 12 de la Ley 1581 del 2012 fija obligaciones estrictas con respecto a la información que debe proporcionarse a los usuarios cuando se procesan sus datos personales. Estas obligaciones no solo deben cumplirse cuando se solicita su consentimiento, sino que también se aplican sin importar el fundamento legal utilizado para procesar los datos (por ejemplo, basados en intereses legítimos o para la ejecución de un contrato).

En concordancia con lo anterior, según la ley de protección de datos personales, el titular del dato debe recibir información fácil de entender, entre otras cosas, sobre las categorías de datos personales que se procesan y la finalidad del procesamiento. En este sentido, a diferencia de la ley general en Europa, conocida como RGPDP (GDPR, por sus siglas en inglés), en la norma colombiana no se menciona explícitamente la toma de decisiones automatizada[90]. Sin embargo, el artículo 12 establece en su literal *a* que es obligación del responsable del tratamiento informar al titular sobre el (los) tratamiento(s) a los que estarán sujetos los datos. Por *tratamiento* se entiende "[c]ualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección,

[89] Michal S. Gal y Niva Elkin-Koren, "Algorithmic Consumers", *Harvard Journal of Law & Technology (Harvard JOLT)* 30, n.º 2 (2016), https://heinonline.org/HOL/Page?handle=hein.journals/hjlt30&id=321&div=&collection=.

[90] Wachter, Mittelstadt y Russell, "Counterfactual Explanations"; Doina Popescu Ljungholm, "Regulation of Automated Individual Decision-Making and Artificially Intelligent Algorithmic Systems: Is the GDPR a Powerful Enough Mechanism to Protect Data Subjects?", *Analysis and Metaphysics*, n.º 17 (2018): 116-122.

almacenamiento, *uso*, circulación o supresión"[91] (énfasis añadido). Además, el magistrado Ciro Angarita, en la sentencia T-414 de 1992, planteó el concepto de perfiles virtuales[92]. En esta providencia se determinó que, por las características propias de los datos, una vez producidos, bien sea de forma manual o por incidencia de una máquina, podrán ser usados, en combinación con otros de procedencias distintas pero adscritos a la misma persona, configurándose el *perfil virtual*. Así, haciendo una interpretación integral, dentro del (los) tratamiento(s) que el responsable debe informar al titular del dato —*consumidor*— se puede inferir que consiste en tratamientos tanto manuales como automatizados, toda vez que la Ley 1581 se entiende como una ley neutral en sentido tecnológico.

No obstante, es difícil materializar estas obligaciones a menos que se inyecte mucha más transparencia en los sistemas y procesos de IA[93]. Se necesitan esfuerzos adicionales para aumentar la transparencia algorítmica y explicar a los consumidores cómo los sistemas y procesos de IA usan sus datos personales, particularmente cuando estos se reutilizan. Por esta razón, es importante que los consumidores no se enfrenten a una avalancha de explicaciones técnicas, sino que necesitan información significativa para comprender realmente las consecuencias de las decisiones automatizadas[94].

En consecuencia, a pesar de las diversas obligaciones que en materia de protección de datos tienen los responsables, es fundamental aclarar que el principio de transparencia, en concordancia con el de explicabilidad de las decisiones —*siguiendo el régimen europeo*—, entra en colisión con el mismo concepto de IA y algoritmos, toda vez que lo que sucede en la caja negra o detrás de los patrones oscuros, en principio no es reconocible o detectable[95]. Es decir, si bien la ley de protección de datos busca que el responsable pueda explicar su *tratamiento o*

[91] Ley Estatutaria 1581/2012, art. 3.

[92] C. Const., Sent. T-414/1992. M.P. Ciro Angarita Barón.

[93] Wachter, Mittelstadt y Floridi, "Why a Right".

[94] Ljungholm, "Regulation of Automated Individual".

[95] Sandra Wachter, "Privacy: Primus Inter Pares-Privacy as a Precondition for Self-Development, Personal Fulfillment and the Free Enjoyment of Fundamental Human Rights", *SSRN Electronic Journal*, n.º 23 (22 de enero del 2017), https://doi.org/10.2139/SSRN.2903514.

decisión, no podrá hacerlo en términos técnicos debido a la naturaleza de la IA y del aprendizaje automático.

Sobre el particular, Sandra Wachter, Brent Mittelstadt y Chris Russell presentan el concepto de *explicaciones contrafácticas incondicionales* como un nuevo tipo de explicación de las decisiones automatizadas que podría resolver muchos de estos problemas[96]. Por un lado, estos autores afirman que este tipo de explicaciones describen las condiciones mínimas que habrían conducido a una decisión alternativa, sin necesidad de describir la lógica completa del algoritmo, lo cual en principio terminaría en una disputa en materia de propiedad intelectual, como se mencionó.

En el modelo de explicaciones contrafácticas, los autores afirman que, en lugar de intentar dar cuenta de todo el razonamiento matemático de un proceso de toma de decisiones muy complejo, debido al uso de algoritmos, los "contrafácticos" permiten ofrecer afirmaciones sencillas sobre lo que tendría que ser diferente en la situación de un individuo para obtener un resultado diferente. Así, este modelo no pretende de ningún modo indicar por qué ha pasado algo, sino que explica lo que ha pasado en el modelo para que así el usuario pueda controvertirlo, si lo desea. Finalmente, los autores establecen tres variables que ejemplifican la información que un titular querría saber cuando es sujeto de decisiones automatizadas: (1) qué pasó: por qué no me dieron el préstamo; (2) qué información existe para poder impugnar la decisión si la considero inexacta o injusta; y (3) aun si la decisión es correcta y justa, qué puedo hacer para mejorar mis posibilidades en el futuro.

Las implicaciones de las decisiones automatizadas en Colombia en relación con la protección de datos merecen una investigación independiente y se salen del objeto de este escrito. Sin embargo, vale la pena tener en cuenta para futuras investigaciones si dentro del principio general de transparencia y responsabilidad demostrada se incluye el derecho a impugnar una decisión de este tipo, y así, por ejemplo, un consumidor podría solicitar una explicación de una decisión por parte de un algoritmo usado por algún responsable del tratamiento de datos, en otras palabras, una explicación de cómo la máquina ha llegado a su resultado.

[96] Sandra Wachter, Brent Mittelstadt y Chris Russell, "Counterfactual Explanations".

Principio de responsabilidad demostrada

El principio de responsabilidad exige que las empresas demuestren que cumplen con las normas de protección de datos. Los responsables y encargados deben implementar medidas técnicas apropiadas para garantizar y poder demostrar que el procesamiento se realiza de acuerdo con la ley[97]. De esta forma, las empresas serán responsables del inadecuado uso de los datos personales, a menos que puedan demostrar que no fueron responsables de ninguna manera del evento que causó el daño. Por lo tanto, las empresas siempre deben poder demostrar que el (los) tratamiento(s) que hace(n) de los datos cumple(n) con las normas de protección de datos, así como con las buenas prácticas empresariales[98]. En este sentido, cabe preguntarse para una futura investigación, si las empresas pueden demostrar que su tecnología de IA cumple con las reglas, especialmente cuando las máquinas se vuelven autónomas y aprenden por sí mismas.

Implicaciones en derecho del consumidor

Algunos autores afirman que la nueva generación de algoritmos potencializa la autonomía del consumidor, incluso en un nivel superior, toda vez que la decisión se toma sobre qué algoritmo usa el consumidor y no sobre el producto que está buscando[99]. Este argumento se basa en

[97] Nelson Remolina Angarita, Manuel Miguel Tenorio y Gustavo Quintero Navas, "De la responsabilidad demostrada en las funciones misionales de la Registraduría Nacional del Estado Civil: Hacia un programa de gestión de datos personales y la consolidación de un buen gobierno corporativo de esa clase de información", Registraduría Nacional del Estado Civil, Centro de Estudios en Democracia y Asuntos Electorales y Remolina Angarita Consultores (Bogotá: Temis, 2018), 116-120, https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/De-la-responsabilidad-demostrada-en-las-funciones-de-la-RNEC-2018-Nelson-Remolina-Angarita1.pdf.

[98] Joseph Alhadeff, Brendan Van Alsenoy y Jos Dumortier, "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions", en *Managing Privacy Through Accountability*, editado por D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland y H. Postigo (Londres: Palgrave Macmillan, 2012), 49-82, https://doi.org/10.1057/9781137032225_4; OECD, *Artificial Intelligence in Society.*

[99] Gal y Elkin-Koren, "Algorithmic Consumers".

que el consumidor intervenga en cualquier paso del proceso de compra, como cambiar los parámetros de decisión del algoritmo —*elegir el color deseado*— para disminuir potencialmente la sugerencia de este. Sin embargo, esta línea argumentativa tiene incidencia en el grado de transparencia del algoritmo, situación que hoy en día no se materializa. Por esta razón, el derecho a recibir información clara y suficiente pareciera incompatible con la necesidad de transparencia y explicabilidad de los algoritmos[100], pues, como se describió, no se conoce cómo llega el algoritmo a esa decisión[101].

En este sentido, la mayor personalización y focalización de los servicios podría disminuir las opciones de los usuarios y dificultar su capacidad de encontrar información que considere significativa para tomar una decisión informada[102]. Cuanto mayor sea la dependencia del individuo respecto de estas tecnologías para tomar una decisión, es menos probable que tenga una opción real. Incluso, los algoritmos pueden llegar a manipular al consumidor en formas que no necesariamente promueven el bienestar. A manera de ejemplo, el controvertido experimento de Facebook en el 2014 sobre contagio emocional consistió en la manipulación de las noticias de más de medio millón de usuarios, para cambiar la cantidad de publicaciones positivas y negativas que vieron[103]. Los investigadores encontraron que los estados de ánimo eran contagiosos, así, las personas que vieron publicaciones positivas respondieron escribiendo publicaciones positivas. Del mismo modo, ver más contenido negativo llevó a los espectadores a ser más negativos en sus publicaciones[104]. Así, los algoritmos tienen un valor significativo a la hora de manipular a los consumidores en línea, toda vez que algunos intentan reemplazar el juicio de valor humano por un código opaco, y

[100] Wachter, Mittelstadt y Floridi, "Why a Right".

[101] Flórez Rojas y Vargas Leal, "El impacto".

[102] Gal, "Algorithmic Challenges".

[103] Vindu Goel, "Facebook Tinkers With Users' Emotions in News Feed Experiment, Stirring Outcry", *The New York Times*, 2014, https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html.

[104] *Ibid*., Hewage *et al*., "Review: Big Data Techniques of Google, Amazon, Facebook and Twitter".

los consumidores son más vulnerables a tal manipulación debido a su incapacidad para descifrar estos algoritmos[105].

De esta forma, es necesario evaluar el impacto en las prácticas comerciales, tales como el *marketing* depredador con IA y el funcionamiento consecuente de los mercados con estas nuevas tecnologías. Para ello, se deben cuestionar diversos conceptos sobre los que se basa el derecho del consumo en Colombia, como el empoderamiento del consumidor por medio de la información y la transparencia[106]. Teniendo presente el concepto de algoritmos deterministas, compras en línea y manipulación en las preferencias de los consumidores, cabe preguntarnos si es realista proteger a los consumidores valiéndose de la información que les proporcionan las empresas, cuando esta está dirigida individualmente a ellos dependiendo del perfil establecido por dichas compañías. En la misma línea, ¿cómo se protegerán los consumidores cuando se enfrenten a resultados discriminatorios de decisiones automatizadas basadas en el uso de IA en Colombia?

Impacto en la regulación de derecho de consumo

Empresas, gobiernos y los mismos consumidores deben afrontar las nuevas formas de publicidad, como el *marketing* de influenciadores y el *marketing* con IA, que potencialmente disminuyen la autonomía del consumidor[107]. En este sentido, puede afirmarse que la idea de autonomía y la libre toma de decisiones está en declive cuando los consumidores no comprenden cómo funciona el mercado o cómo se han generado las

[105] Gal, "Algorithmic Challenges".

[106] Nelson Remolina Angarita y María Lorena Florez Rojas, "Consumidor y comercio electrónico", en *Derecho del consumo: Problemáticas actuales* (Bogotá: Ibáñez-Universidad Santo Tomás, 2013).

[107] Marijke De Veirman, Veroline Cauberghe y Liselot Hudders, "Marketing Through Instagram Influencers: The Impact of Number of Followers and Product Divergence on Brand Attitude", *International Journal of Advertising* 36, n.º 5 (2017): 798-828, https://doi.org/10.1080/02650487.2017.1348035; Dominique Hanssens, Daniel Thorpe y Carl Finkbeiner, "Marketing When Customer Equity Matters", *Harvard Business Review* 86, n.º 5 (2008): 117-123, https://hbr.org/2008/05/marketing-when-customer-equity-matters.

ofertas que reciben[108]. En este orden de ideas, se analiza si la Ley 1480 del 2011 cobija estas prácticas en donde los consumidores a menudo desconocen las restricciones que estas tecnologías presentan, como, por ejemplo, cuando no saben que el precio de un producto puede estar determinado en función de su perfilamiento[109].

La Ley 1480 del 2011 establece que la información constituye un elemento de importancia trascendente, pues es un medio para que el consumidor pueda ejercer y hacer efectivos sus derechos. De tal manera, la información que se brinde al consumidor sobre los bienes y servicios ofrecidos debe ser clara, veraz y suficiente, y queda prohibido todo tipo de publicidad engañosa[110]. Por un lado, los artículos 3 y 5 señalan de forma general que los consumidores en Colombia tienen derecho a recibir información completa y transparente sobre los productos que se ofrezcan, así como sobre los riesgos que puedan derivarse del consumo o utilización de estos[111]. Así, de la lectura de los artículos se pueden desprender dos posibles situaciones.

La primera considera a la plataforma digital un producto en sí mismo, por tanto, debe informar al consumidor una vez este acceda a ella, indicándole que su perfil de usuario es analizado por algoritmos para *enviar recomendaciones y mejorar el proceso de compra*. Del mismo modo, el proveedor deberá poner de presente los riesgos asociados al uso de estos algoritmos, para que el consumidor "informado", decida si entra o no a la plataforma. Sin embargo, la segunda situación —que es la más común—, trata a la plataforma no como un producto, sino como el medio para ofrecer otros productos. Por ende, el proveedor de la plataforma tecnológica no tendría la obligación de informar previamente al consumidor que su perfil es usado para alimentar el algoritmo y, en consecuencia, tanto productos como precios pueden variar de consumidor a consumidor.

[108] Frederik Zuiderveen Borgesius y Joost Poort, "Online Price Discrimination".

[109] Richards, Liaukonyte y Streletskaya, "Personalized Pricing".

[110] Juan Carlos Villalba Cuellar, *Introducción al derecho del consumo* (Bogotá: Universidad Militar Nueva Granada, 2012).

[111] Ley 1480 del 2011, 12 de octubre del 2011, por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones, http://www.secretariasenado.gov.co/senado/basedoc/ley_1480_2011.html.

Por otro lado, si analizamos el contenido del artículo 26 sobre información pública de precios, se establece que el proveedor está obligado a informar al consumidor el precio de venta al público, incluidos todos los impuestos y costos adicionales de los productos. En este sentido, la norma tal y cómo está redactada no implica en ningún sentido que el proveedor deba informar al consumidor que el precio de un producto puede variar dependiendo del perfilamiento del usuario. Un ejemplo de lo anterior se materializa en las diversas funciones que tienen las tarjetas de fidelización, con las cuales los consumidores reciben recompensas y descuentos "gratuitos" a cambio de información sobre ellos[112].

De esta forma, las normas del Estatuto del Consumidor que se ocupan de los requisitos de información precontractual pueden llegar a perder vigencia, en la medida en que cada vez existen más productos y servicios que se ejecutan con algoritmos. Según las normas actuales, los consumidores tienen derecho a recibir información esencial sobre el producto o servicio, por ejemplo, sus características o su precio. Sin embargo, la legislación colombiana no establece elementos de información sobre el proceso de decisiones automatizadas por medio de algoritmos de IA, precios individuales o dinámicos. La Ley 1480 del 2011 y sus decretos reglamentarios no establecen una obligación de informar al consumidor sobre la importancia relativa de los parámetros de clasificación y las razones por las cuales se eligieron esos criterios, así como tampoco es obligación de los empresarios informar sobre el uso de algoritmos subyacentes que influyen en el proceso de compra del consumidor.

Por las razones expuestas, es indispensable el papel del derecho de consumo en el desarrollo de un marco legal de IA en el país. Es posible que, gracias a la jurisprudencia, la lectura del Estatuto del Consumidor se extienda a espacios en donde el uso de la IA es la norma y no la excepción, adoptando la primera lectura mencionada, con miras a garantizar que los consumidores obtengan información precisa y confiable sobre la naturaleza del modelo comercial y de la oferta específica. A partir de una lectura extensiva de la norma se puede afirmar que el uso de algoritmos para la creación de perfiles virtuales con miras a crear precios

[112] Gregory E. Smith y Michael S. Rimler, "Will You Be Mined? Ethical Considerations of Opt-in Loyal Programs and Price Discrimination", *Information Systems*, n.º 2 (2009), https://doi.org/10.48009/2_iis_2009_204-209.

diferenciadores, ofertas y publicidad dependiendo del consumidor se enmarca en lo que el proveedor o productor debe informar al consumidor a la hora de ofrecer sus productos. No obstante, se resalta que esa obligación no es tan clara para los proveedores hoy en día, y no se obtiene este tipo de información cuando se accede a una plataforma web.

Conclusiones

La intersección entre la tecnología y la sociedad no es solo una herramienta para mejorar la calidad de vida y la eficiencia en el comercio electrónico; es igualmente el siguiente paso en la evolución del consumidor tradicional a uno guiado por algoritmos. En este capítulo se considera que a esta etapa se debe llegar informado y preparado institucionalmente. Los continuos avances en IA ofrecen parcialmente —pero dispondrán a totalidad— la capacidad prometida de autonomía tecnológica. De esta forma, ajustarse a la idea de que un consumidor en la web se traduce en un perfil virtual e incluso puede llegar a convertirse en un agente algorítmico suena algo hollywoodense, pero está más cerca de lo que pensamos. Hoy en día, los consumidores conviven con algoritmos que monitorean su entorno, para luego aprender y analizar la información recibida para generar recomendaciones y perfiles de compra.

La IA y, en general, cualquier tecnología disruptiva forman parte de un área en la que muchos sectores están tratando de trabajar juntos, incluso en las áreas cruciales de la equidad, la transparencia y la responsabilidad en la toma de decisiones algorítmicas. De esta forma, es necesario un enfoque de múltiples partes interesadas. Así, el derecho y la ética desempeñan un papel importante. La opacidad, la imprevisibilidad de la IA y su naturaleza potencialmente discriminatoria exigen que pensemos en las implicaciones legales y éticas desde el principio.

Si bien, de cierta forma, la protección de datos proporciona los límites para la recopilación y el procesamiento de datos del consumidor con el fin de ofrecer soluciones o productos de IA, la ley del consumidor puede llegar a garantizar que este comprenda las implicaciones de dichas tecnologías y el resultado de las decisiones tomadas por las tecnologías de aprendizaje automático. Además de eso, una ley del consumidor clara y moderna puede ayudar a que los diversos desarrollos tecnológicos de IA crezcan en el país, toda vez que, si no hay transparencia sobre el uso

de productos que se ejecutan en algoritmos, la confianza de los consumidores en los productos de IA se verá afectada negativamente. En consonancia, el país debe contar con un mapeo detallado y una evaluación cuidadosa de todo el acervo de la ley del consumidor en general, así como las normas específicas del sector, en particular industrias como servicios de salud, financieros y de energía para verificar si estos marcos legales son adecuados para la aplicación de decisiones automatizadas con uso de IA.

Algunas recomendaciones generales para la implementación del uso de IA en el comercio electrónico se esbozan a lo largo del texto, pero se pueden sintetizar en las siguientes:

- Los productos y servicios basados en IA deben ser fáciles de usar y cumplir legalmente de forma predeterminada, evitando la discriminación algorítmica y la falta de transparencia o privacidad.
- Debe existir el derecho de objetar la toma de decisiones automatizadas y de impugnarla. Los usuarios deben tener derecho a la transparencia sobre en qué parámetros se basan las ofertas y cómo la máquina ha llegado a su resultado.
- La implementación de productos de IA debe desarrollarse y utilizarse respetando plenamente las normas de protección de datos, teniendo en cuenta los principios de equidad, transparencia, limitación de propósito, minimización de datos, responsabilidad y responsabilidad demostrada. Así, no se debe olvidar que el potencial de los algoritmos para transformar la sociedad es enorme, por lo que garantizar una relación más rápida y reflexiva de lo normal entre estos sectores es absolutamente fundamental.

Bibliografía

Alba, Joseph, John Lynch, Barton Weitz, Chris Janiszewski, Richard Lutz, Alan Sawyer y Stacy Wood. "Interactive home shopping: Consumer, retailer, and manufacturer incentives to participate in electronic market places". *Journal of Marketing* 61, n.º 3 (2 de julio de 1997): 38-53. https://doi.org/10.1177/002224299706100303.

Alhadeff, Joseph, Brendan Van Alsenoy y Jos Dumortier. "The accountability principle in data protection regulation: Origin, development and

future directions". En *Managing privacy through accountability*, editado por D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland y H. Postigo, 49-82. Londres: Palgrave Macmillan, 2012. https://doi.org/10.1057/9781137032225_4.

André, Quentin, Ziv Carmon, Klaus Wertenbroch, Alia Crum, Douglas Frank, William Goldstein, Joel Huber, Leaf van Boven, Bernd Weber y Haiyang Yang. "Consumer choice and autonomy in the age of artificial intelligence and big data". *Customer Needs and Solutions* 5, n.os 1-2 (marzo del 2018): 28-37. https://doi.org/10.1007/s40547-017-0085-8.

Barocas, Solon, Sophie Hood y Malte Ziewitz. "Governing algorithms: A provocation piece". *Pat. & Trademark Off. Soc'y*, n.º 69 (10 de abril de 1987). https://doi.org/10.2139/ssrn.2245322.

Bathaee, Yavar. "Artificial intelligence opinion liability". *Berkeley Technology Law Journal* 35, n.º 1 (2020): 113. https://doi.org/10.15779/Z38P55DH32.

Baye, Michael R., John Morgan y Patrick Scholten. "The value of information in an online consumer electronics market". *Journal of Public Policy and Marketing* 22, n.º 1 (2003): 17-25. https://doi.org/10.1509/jppm.22.1.17.17625.

Big Data Value Association (BDVA), "Data-driven artificial intelligence for European economic competitiveness and societal progress-position statement", 2018.

Beck, Estee N. "The invisible digital identity: Assemblages in digital networks". *Computers and Composition* 35 (1.º de marzo del 2015): 125-140. https://doi.org/10.1016/J.COMPCOM.2015.01.005.

Benohr, Iris. *EU Consumer law and human rights*. Oxford Studies in European Law. Oxford, Nueva York: Oxford University Press, 2014. https://global.oup.com/academic/product/eu-consumer-law-and-human-rights-9780199651979?cc=us&lang=en&.

Borgesius, Frederik Zuiderveen y Joost Poort. "Online price discrimination and EU data privacy law". *Journal of Consumer Policy* 40, n.º 3 (2017): 347-366. https://doi.org/10.1007/s10603-017-9354-z.

Cheah, P. H., R. Zhang, H. B. Gooi, H. Yu y M. K. Foo. "Consumer energy portal and home energy management system for smart grid applications". *10th International Power and Energy Conference, IPEC 2012*, 407-411. 2012. https://doi.org/10.1109/ASSCC.2012.6523302.

Cirucci, M. Angela y Barry Vacker. "*Black mirror" and critical media theory*. Rowman & Littlefield, 2018. https://books.google.com.co/books?hl=en&lr=&id=UkNsDwAAQBAJ&oi=fnd&pg=PR5&dq=black+mirror+implications+in+social+life&ots=QnNWlYHb8e&sig=6xY5JxiHOAgqEH

N-JeTSEH83z-8&redir_esc=y#v=onepage&q=black mirror implications in social life&f=false.

Coeckelbergh, Mark. "Artificial intelligence, responsibility attribution, and a relational justification of explainability". *Science and Engineering Ethics* (24 de octubre del 2019): 1-18. https://doi.org/10.1007/s11948-019-00146-8.

Council of Europe. "Human rights guidelines for internet service providers". Council of Europe, 2008.

Courtois, Cédric y Elisabeth Timmermans. "Cracking the Tinder code: An experience sampling approach to the dynamics and impact of platform governing algorithms". *Journal of Computer-Mediated Communication* 23, n.º 1 (1.º de enero del 2018): 1-16. https://doi.org/10.1093/jcmc/zmx001.

Dignum, Virginia. "Ethics in artificial intelligence: Introduction to the special issue". *Ethics and Information Technology* 20, n.º 1 (1.º de marzo del 2018): 1-3. https://doi.org/10.1007/s10676-018-9450-z.

Dowek, Gilles y Jean-Jacques Lévy. *Introduction to the theory of programming*. Londres: Springer-Verlag, 2011. https://www.springer.com/gp/book/9780857290755.

Duarte, Fernando. "5 algoritmos que ya están tomando decisiones sobre tu vida y que quizás tú no sabías". *BBC News Mundo*, 2018. https://www.bbc.com/mundo/noticias-42916502.

Duhigg, Charles. "How companies learn your secrets". *The New York Times*, 2012. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

Elliott, Justin y Luca Waldron, "Here's how TurboTax just tricked you into paying to file your taxes—ProPublica", 2019. https://www.propublica.org/article/turbotax-just-tricked-you-into-paying-to-file-your-taxes.

European Commission, "Communication from the Commission to the European Parliament: Artificial intelligence for Europe". Bruselas, 2018.

— "Inteligencia artificial: Un enfoque europeo orientado a la excelencia y la confianza". Bruselas, 2020. https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_es.pdf.

Flórez Rojas, María Lorena. "Are online consumers protected from geo-blocking practices within the European Union?". *International Journal of Law and Information Technology* 26, n.º 2 (2018). https://doi.org/10.1093/ijlit/eay004.

— "Legal uncertainty: Proposed regulation on addressing geo-blocking". En *Managing Risk in the Digital Society: Proceedings of the 13th International Conference on Internet, Law & Politics Universitat Oberta de*

Catalunya, coordinado por B. Anglés, J. Balcells, A. M. Delgado García, M. Fiori, M. Julià, A. Mantelero, C. Marsan, M. J. Pifarré y M. Vilasau, 305-319. Barcelona: Huygens, 2017.

Flórez Rojas, María Lorena, y Juliana Vargas Leal. "El impacto de las herramientas de inteligencia artificial: Un análisis en el sector público en Colombia". En Carolina Aguerre *et al., Inteligencia artificial en América Latina y el Caribe: Ética, gobernanza y políticas*. 2020. https://guia.ai/wp-content/uploads/2020/05/GECTI-El-impacto-de-herramientas-de-inteligencia-artificial.pdf.

Floridi, Luciano. *The Fourth Revolution: How the infosphere is reshaping human reality*. Londres: Oxford University Press, 2014. https://www.oii.ox.ac.uk/research/books/the-fourth-revolution/.

Fornasier, Mateus de Oliveira. "The applicability of the internet of things (IoT) between fundamental rights to health and to privacy". *Revista de Investigações Constitucionais* 6, n.º 2 (31 de enero del 2020): 297-321. https://doi.org/10.5380/RINC.V6I2.67592.

Frank, Xavier. "Is Watson for Oncology per se unreasonably dangerous?: Making a case for how to prove products liability based on a flawed artificial intelligence design". *American Journal of Law & Medicine* 45, n.os 2-3 (1.º de mayo del 2019): 273-294. https://doi.org/10.1177/0098858819871109.

Gal, Michal S. "Algorithmic challenges to autonomous choice". *Mich. Telecomm. & Tech. L. Rev*, n.º 25 (2018). https://doi.org/10.2139/ssrn.2971456.

Gal, Michal S. y Niva Elkin-Koren. "Algorithmic consumers". *Harvard Journal of Law & Technology (Harvard JOLT)* 30, n.º 2 (2016). https://heinonline.org/HOL/Page?handle=hein.journals/hjlt30&id=321&div=&collection=.

Garcia, Megan. "Racist in the machine: The disturbing implications of algorithmic bias". *World Policy Journal* 33, n.º 4 (2016): 111-117. https://muse.jhu.edu/article/645268/summary.

Goel, Vindu. "Facebook tinkers with users' emotions in news feed experiment, stirring outcry". *The New York Times*, 2014. https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html.

Gran, Anne Britt, Peter Booth y Taina Bucher. "To be or not to be algorithm aware: A question of a new digital divide?". *Information Communication and Society* 1790, n.º 24 (2020): 12. https://doi.org/10.1080/1369118X.2020.1736124.

Gray, Colin M., Yubo Kou, Bryan Battles, Joseph Hoggatt y Austin L Toombs. "The dark (patterns) side of UX design". En *Proceedings of the 2018 CHI*

Conference on Human Factors in Computing Systems. Nueva York: ACM, 2018. https://doi.org/10.1145/3173574.3174108.

Hanssens, Dominique, Daniel Thorpe y Carl Finkbeiner. "Marketing When Customer Equity Matters". *Harvard Business Review* 86, n.º 5 (2008): 117-123. https://hbr.org/2008/05/marketing-when-customer-equity-matters.

He, Minghua, Nicholas R Jennings y Ho-Fung Leung. "On Agent-Mediated Electronic Commerce" 15, n.º 4 (2003): 985-990.

Hewage, Thulara N., Malka N. Halgamuge, Ali Syed y Gullu Ekici. "Review: Big Data Techniques of Google, Amazon, Facebook and Twitter". *Journal of Communications* 13, n.º 2 (February 1, 2018): 94-100. https://doi.org/10.12720/jcm.13.2.94-100.

High Level Independent Group on Artificial Intelligence (AI HLEG). *Ethics guidelines for trustworthy AI*. European Commission, 2019.

Hill, Jonathan. *Cross-border consumer contracts*. Oxford Private International Law Series. Oxford, Nueva York: Oxford University Press, 2008. https://global.oup.com/academic/product/cross-border-consumer-contracts-9780199276547?cc=it&lang=en&.

Hill, Kashmir. "The secretive company that might end privacy as we know it". *The New York Times*, 2020. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Hurwitz, Judith y Daniel Kirsch. *Machine learning IBM limited edition*. Nueva Jersey: John Wiley & Sons, 2018. http://www.wiley.com/go/permissions.

Kramer, Adam D. I., Jamie E. Guillory y Jeffrey T. Hancock. "Experimental evidence of massive-scale emotional contagion through social networks". *Proceedings of the National Academy of Sciences of the United States of America* 111, n.º 24 (17 de junio del 2014): 8788-8790. https://doi.org/10.1073/pnas.1320040111.

Lee, Hee Andy, Rob Law y Jamie Murphy. "Helpful reviewers in TripAdvisor, an online travel community". *Journal of Travel and Tourism Marketing* 28, n.º 7 (octubre del 2011): 675-688. https://doi.org/10.1080/10548408.2011.611739.

Letschert, Rianne, Lorena Sosa, Conny Rijken y G. M. F. Römkens. *Feasibility study to assess the possibilities, opportunities and needs to standardise national legislation on violence against women, violence against children and sexual orientation violence.* Bruselas: European Commission, 2010. https://pure.uvt.nl/portal/files/1371655/Letschert_Identifying_minimum_standards_in_the_field_of_violence_111205_publishers_immediately.pdf.

Ley 1480 del 2011, 12 de octubre del 2011, por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones. http://www.secretariasenado.gov.co/senado/basedoc/ley_1480_2011.html.

Ley Estatutaria 1581 del 2012, 17 de octubre del 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

Li, Xiaocheng, Liu Xin, Zhang Zengjie, Xia Yongming y Qian Songrong "Design of healthy eating system based on web data mining". En *Proceedings-2010 WASE International Conference on Information Engineering*, 346-349, *ICIE*, 2010. https://doi.org/10.1109/ICIE.2010.89.

Ljungholm, Doina Popescu. "Regulation of automated individual decision-making and artificially intelligent algorithmic systems: Is the GDPR a powerful enough mechanism to protect data subjects?". *Analysis and Metaphysics*, n.º 17 (2018): 116-122.

Lu, Donna. "Face up to reality". *New Scientist* 245, n.º 3267 (1.º de febrero del 2020): 23. https://doi.org/10.1016/s0262-4079(20)30212-8.

Lynch, John G. y Dan Ariely. "Competition on price, quality, and distribution". *Marketing Science* 19, n.º 1 (2000): 83-103. www.bizrate.com.

Maccioni, Antonio y Riccardo Torlone. "Kayak: A framework for just-in-time data preparation in a data lake". En *Advanced Information Systems Engineering*, editado por Bo Steinholtz, Arne Sølvberg y Lars Bergman, 474-489. Springer Verlag, 2018. https://doi.org/10.1007/978-3-319-91563-0_29.

MacIntyre, A. C. "Determinism". *Mind* 66, n.º 261 (1957): 28-41. https://www.jstor.org/stable/2251366.

Maggiolino, Mariateresa. "EU trade secrets law and algorithmic transparency". *Bocconi Legal Studies Research*, n.º 27 (22 de abril del 2019). https://doi.org/10.2139/ssrn.3363178.

Mann, Monique y Tobias Matzner. "Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination". *Big Data & Society* 6, n.º 2 (16 de julio del 2019): 1-11. 205395171989580. https://doi.org/10.1177/2053951719895805.

Mathur, Arunesh, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty y Arvind Narayanan. "Dark patterns at scale: Findings from a crawl of 11K shopping websites". *Proceedings of the ACM on human-computer interaction*. Association for Computing Machinery, 1.º de noviembre del 2019. https://doi.org/10.1145/3359183.

McCarthy, John, Marvin L. Minsky, Nathaniel Rochester y Claude E. Shannon. "A proposal for the Dartmouth Summer Research Project on Artificial

Intelligence, August 31, 1955". *AI Magazine* 27, n.º 4 (15 de diciembre del 2006): 12. https://doi.org/10.1609/AIMAG.V27I4.1904.

McCulloch, Warren S. y Walter Pitts. "A logical calculus of the ideas immanent in nervous activity". *Bulletin of Mathematical Biophysics* 52, n.º 2 (1990): 99-115.

McKenna, Eoghan, Ian Richardson y Murray Thomson. "Smart Meter Data: Balancing consumer privacy concerns with legitimate applications". *Energy Policy* 41 (1.º de febrero del 2012): 807-814. https://doi.org/10.1016/j.enpol.2011.11.049.

McNicholas, Chris, Derek Bell y Julie Reed. "Opening the 'black box' of plan-do-study-act cycles: Achieving a scientific yet pragmatic approach to improving patient care". *BMJ Quality & Safety* 23, n.º 4 (1.º de abril del 2014): 352-352. https://doi.org/10.1136/bmjqs-2014-002893.11.

Meissner, Christian A. y John C. Brigham. "Thirty years of investigating the own-race bias in memory for faces: A meta-analytic review". *Psychology, Public Policy, and Law* 7, n.º 1 (2001): 3-35. https://doi.org/10.1037/1076-8971.7.1.3.

Milossi, Maria; Eugenia Alexandropoulou-Egyptiadouy Konstantinos Psannis. "AI ethics: Algorithmic determinism or self-determination? The GPDR Approach". *IEEE Internet Computing*, n.º 9 (2021): 1-12. https://doi.org/10.1109.

Mittelstadt, Brent Daniel, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter y Luciano Floridi. "The ethics of algorithms: Mapping the debate". *Big Data & Society* 3, n.º 2 (1.º de diciembre del 2016). https://doi.org/10.1177/2053951716679679.

Modugno, Chiara y Tonny Krijnen. "Through the *Black mirror*: Discourses on gender and technology in popular culture". *Catalan Journal of Communication & Cultural Studies* 12, n.º 1 (19 de mayo del 2020): 3-19. https://doi.org/10.1386/cjcs_00011_1.

Monasterio Astobiza, Aníbal. "Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos". *Dilemata* 9, n.º 24 (2017): 185-217. https://doi.org/1989-7022.

Mu, Li. "Russian neural networks predict Donald Trump will be next US president". En *ImageNet Large Scale Visual Recognition Challenge 2016 (ILSVRC2016)*, 2016. https://www.ewdn.com/2016/08/08/neural-networks-see-donald-trump-as-us-president/.

Mueller, Milton L., Yuri Park, Jongsu Lee y Tai Yoo Kim. "Digital identity: How users value the attributes of online identifiers". *Information Economics*

and Policy 18, n.º 4 (1.º de noviembre del 2006): 405-422. https://doi.org/10.1016/J.INFOECOPOL.2006.04.002.

Narayanan, Arvind, Arunesh Mathur, Marshini Chetty y Mihir Kshirsagar. "Dark patterns: Past, present, and future the evolution of tricky user interfaces". *Communications of the ACM* 63, n.º 9 (2020): 42-47. https://doi.org/10.1145/3397884.

Natale, Simone y Andrea Ballatore. "Imagining the thinking machine: Technological myths and the rise of artificial intelligence". *Convergence* 26, n.º 1 (1.º de febrero del 2020): 3-18. https://doi.org/10.1177/1354856517715164.

Nilashi, Mehrbakhsh, Othman Ibrahim, Elaheh Yadegaridehkordi, Sarminah Samad, Elnaz Akbari y Azar Alizadeh. "Travelers decision making using online review in social network sites: A case on TripAdvisor". *Journal of Computational Science* 28 (1.º de septiembre del 2018): 168-179. https://doi.org/10.1016/j.jocs.2018.09.006.

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) y Organización de las Naciones Unidas (ONU). *Declaración sobre la Utilización del Progreso Científico y Tecnológico en Interés de la Paz y en Beneficio de la Humanidad*. 1975. https://www.ohchr.org/SP/ProfessionalInterest/Pages/ScientificAndTechnologicalProgress.aspx.

Organisation for Economic Co-operation and Development (OECD). *Artificial Intelligence in Society*. París: OECD, 2019. https://doi.org/10.1787/eedfee77-en.

Payne, John W., James R. Bettman y Eric J. Johnson. "Adaptive strategy selection in decision making". *Journal of Experimental Psychology: Learning, Memory, and Cognition* 14, n.º 3 (1988): 534-552. https://doi.org/10.1037/0278-7393.14.3.534.

Polonski, Slava. "Algorithmic determinism and the limits of artificial intelligence". *Oxford Internet Institute Blog*, 2016. https://www.oii.ox.ac.uk/blog/algorithmic-determinism-and-the-limits-of-artificial-intelligence/.

Red Iberoamericana de Protección de Datos (RIPD). *Recomendaciones generales para el tratamiento de datos personales en la inteligencia artificial*. 2019. https://www.sic.gov.co/sites/default/files/files/pdf/1.

Remolina Angarita, Nelson, Manuel Miguel Tenorio y Gustavo Quintero Navas. "De la responsabilidad demostrada en las funciones misionales de la Registraduría Nacional del Estado Civil: Hacia un programa de gestión de datos personales y la consolidación de un buen gobierno corporativo de esa clase de información", Registraduría Nacional del Estado Civil, Centro de Estudios en Democracia y Asuntos Electorales y Remolina Angarita

Consultores. Bogotá: Temis, 2018. https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/De-la-responsabilidad-demostrada-en-las-funciones-de-la-RNEC-2018-Nelson-Remolina-Angarita1.pdf.2018.

Remolina Angarita, Nelson y María Lorena Flórez Rojas. "Consumidor y comercio electrónico". En *Derecho del consumo: Problemáticas actuales*. Bogotá: Ibáñez/Universidad Santo Tomás, 2013.

Renda, Andrea. "Artificial intelligence ethics, governance and policy challenges report of a CEPS task force" (Bruselas, 2019), https://www.ceps.eu/wp-content/uploads/2018/03/AI_TFR.pdf.

Richards, Timothy J., Jura Liaukonyte y Nadia A. Streletskaya. "Personalized pricing and price fairness". *International Journal of Industrial Organization* 44 (1.º de enero del 2016): 138-153. https://doi.org/10.1016/j.ijindorg.2015.11.004.

Robinson, Tasha. "*Black Mirror*'s third season opens with a vicious take on social media". *The Verge*, 2016. https://www.theverge.com/2016/10/24/13379204/black-mirror-season-3-episode-1-nosedive-recap.

Samuel, Arthur. "In memoriam-Arthur Samuel: Pioneer in machine learning". *AI Magazine* 11 (15 de septiembre de 1990). https://doi.org/10.1609/AIMAG.V11I3.840.

Samuel, Arthur L. "Some studies in machine learning using the game of checkers. II-Recent Progress", s. d.

Schiek, Dagmar y Victoria Chege. *European Union Non-Discrimination Law: Comparative perspectives on multidimensional equality law*. Oxford, Routledge, 2009. https://books.google.de/books?id=y5np7xd90ioC.

Schreer, George E., Saundra Smith y Kirsten Thomas. "'Shopping while black': Examining racial discrimination in a retail setting". *Journal of Applied Social Psychology* 39, n.º 6 (1.º de junio del 2009): 1432-1444. https://doi.org/10.1111/j.1559-1816.2009.00489.x.

Shugan, Steven M. "The cost of thinking". *Journal of Consumer Research* 7, n.º 2 (1980): 99-111. https://doi.org/10.2307/2489077.

Simonite, Tom. "When it comes to gorillas, Google Photos remains blind". *Wired*, 2018. https://www.wired.com/story/when-it-comes-to-gorillas-google-photos-remains-blind/.

Smith, Gregory E. y Michael S. Rimler. "Will you be mined? Ethical considerations of opt-in loyal programs and price discrimination". *Information Systems*, n.º 2 (2009). https://doi.org/10.48009/2_iis_2009_204-209.

Sobel, Benjamin. "HiQ v. LinkedIn, Clearview AI, and a new common law of web scraping". *SSRN Electronic Journal*, n.º 25 (19 de mayo del 2020). https://doi.org/10.2139/ssrn.3581844.

Steppe, Richard. "Online price discrimination and personal data: A general data protection regulation perspective". *Computer Law and Security Review* 33, n.º 6 (1.º de diciembre del 2017): 768-785. https://doi.org/10.1016/j.clsr.2017.05.008.

Strickland, Eliza. "IBM Watson, heal thyself: How IBM overpromised and underdelivered on AI health care". *IEEE Spectrum* 56, n.º 4 (1.º de abril del 2019): 24-31. https://doi.org/10.1109/MSPEC.2019.8678513.

Trimble, Marketa. "Geoblocking and 'legitimate trade'". En *Intellectual property and obstacles to legitimate trade*, editado por Heath Christopher, Anselm Kamperman y Anke Moerland. US: Wolters Kluwer, 2018. https://papers.ssrn.com/abstract=3135036.

Turing, Alan M. "Computing machinery and intelligence". *Mind*, n.º 49 (1950).

Varian, Hal R. "Beyond big data". *Business Economics* 49, n.º 1 (7 de enero del 2014): 27-31. https://doi.org/10.1057/be.2014.1.

Veirman, Marijke de, Veroline Cauberghe y Liselot Hudders. "Marketing through Instagram influencers: The impact of number of followers and product divergence on brand attitude". *International Journal of Advertising* 36, n.º 5 (2017): 798-828. https://doi.org/10.1080/02650487.2017.1348035.

Verbraucherzentrale. *Geo-Blocking—Tearing down borders for digital content*. Alemania: The Federation of German Consumer Organisations, 2017. https://www.vzbv.de/sites/default/files/2017_vzbv_factsheet_geoblocking_digital_content_1.pdf.

Villalba Cuellar, Juan Carlos. *Introducción al derecho del consumo*. Bogotá: Universidad Militar Nueva Granada, 2012.

Vincent, Alice. "'Black Mirror' is coming true in China, where your 'rating' affects your home, transport and social circle". *The Telegraph*, 2017. https://www.telegraph.co.uk/on-demand/2017/12/15/black-mirror-coming-true-china-rating-affects-home-transport/.

Viola, Roberto. "Artificial intelligence, real benefits". Bruselas, 2018. https://ec.europa.eu/digital-single-market/en/news/artificial-intelligence-real-benefits.

Viswanathan, Siva, Jason Kuruzovich, Sanjay Gosain y Ritu Agarwal. "Online infomediaries and price discrimination: Evidence from the automotive retailing sector". *Journal of Marketing* 71, n.º 3 (2 de julio del 2007): 89-107. https://doi.org/10.1509/jmkg.71.3.089.

Wachter, Sandra. "Privacy: Primus inter pares-privacy as a precondition for self-development, personal fulfillment and the free enjoyment of fundamental

human rights". *SSRN Electronic Journal* (22 de enero del 2017). https://doi.org/10.2139/SSRN.2903514.

Wachter, Sandra, Brent Mittelstadt y Chris Russell. "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR". *Harvard Journal of Law & Technology* 31, n.º 2 (6 de octubre del 2018). https://doi.org/10.2139/SSRN.3063289.

Wachter, Sandra, Brent Mittelstadt y Luciano Floridi. "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation". *International Data Privacy Law* 7, n.º 2 (2017): 76. http://social.cs.uiuc.edu/papers/pdfs/ICA2014-Sandvig.pdf.

Wertenbroch, Klaus, Rom Y. Schrift, Joseph W. Alba, Alixandra Barasch, Amit Bhattacharjee, Markus Giesler, Joshua Knobe *et al.* "Autonomy in consumer choice", *Mark Lett*, n.º 31, 429-439 (2020). Acceso, 1.º de julio del 2021. https://doi.org/10.1007/s11002-020-09521-z.

World Intellectual Property Organization (WIPO). *WIPO technology trends 2019-artificial intelligence*. Suiza, 2019. https://doi.org/978-92-805-3007-0.

Zerilli, John, Alistair Knott, James Maclaurin, Colin Gavaghan y J. Zerilli. "Algorithmic Decision-Making and the Control Problem". *Minds and Machines*, n.º 29 (2019): 555-578. https://doi.org/10.1007/s11023-019-09513-7.

Zuiderveen Borgesius, Frederik y Joost Poort. "Online price discrimination and EU Data Privacy Law". *Journal of Consumer Policy* 40, n.º 3 (1.º de septiembre del 2017): 347-366. https://doi.org/10.1007/s10603-017-9354-z.

Jurisprudencia

C. Const., Sent. T-414/1992. M.P. Ciro Angarita Barón.

Sobre los autores

Jeimy J. Cano M.: Ingeniero y magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes (Bogotá, Colombia). Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Doctor en Administración de Empresas por Newport University (California, Estados Unidos) y doctor en Educación por la Universidad Santo Tomás (Bogotá, Colombia). Miembro fundador del Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes. Tiene más de veinticinco años de experiencia como ejecutivo, académico y profesional en las áreas de seguridad de la información, ciberseguridad, ciencia forense digital, delincuencia digital, privacidad y auditoría de TI. A la fecha es profesor universitario y consultor internacional independiente.

María Lorena Flórez Rojas: Doctora *cum laude* en Derecho por la Scuola Superiore Sant'Anna, Italia. Magíster en Derecho y Tecnologías por la Universidad de Tilburgo, Holanda. Abogada por la Universidad de los Andes (Bogotá, Colombia). Actualmente se desempeña como profesora en la Facultad de Derecho de la Universidad de los Andes y es la directora del GECTI y del Observatorio de Protección de Datos, así como investigadora del grupo Cinfonia de la misma Universidad.

Catalina Guío Español: Abogada *cum laude* por la Universidad de los Andes (Bogotá, Colombia) y especialista en Derecho Financiero por la misma institución. Magíster en Derecho por la Universidad de Harvard (2012) con énfasis en Finanzas Internacionales. Ha participado en procesos de fusión y adquisición de entidades financieras y no financieras y asesorado a diferentes entidades financieras en asuntos regulatorios y del mercado de capitales. Como superintendente delegada de Procedimientos Mercantiles en la Superintendencia de Sociedades de Colombia lideró el único tribunal especializado en Latinoamérica para la resolución de

conflictos societarios. En el 2019 se graduó del programa Sloan Fellows MBA en el MIT Sloan School of Management, donde enfocó sus estudios en finanzas, liderazgo global e innovación. Actualmente se desempeña como directora jurídica de innovación del Banco Davivienda.

Paula Gutiérrez Arboleda: Economista por la Universidad de los Andes. Especialista en Negocios Internacionales y Mercados de Capital por Columbia University, NY (Estados Unidos), magíster en Dirección Comercial y Marketing por la Escuela de Negocios de la Cámara de Comercio de Valladolid (España). Magíster en Integración Europea por la Universidad de Valladolid. Más de quince años de experiencia como consultora y formadora en políticas de ciberseguridad y protección de datos en empresas del sector privado español. Programa Ejecutivo Integral Data Protection Officer acorde a esquema de la Agencia Española de Protección de Datos (AEPD). Doctoranda en Derecho Tecnológico en la Universidad de Valladolid (España). A la fecha es directora operativa de NQA Certificación Colombia.

Carolina Herrera Hincapié: Abogada por la Universidad de los Andes y especialista en Derecho de los Negocios Internacionales por la misma institución. Actualmente se encuentra en el proceso de realizar una maestría en Derecho, Ciencia y Tecnología en la Universidad de Stanford (Estados Unidos). Es miembro del GECTI desde el 2018. Ha trabajado como especialista legal de Microsoft en Colombia y como asociada de la firma Dentons Cárdenas & Cárdenas para el área de Privacidad y Tecnología.

José Fernando Sandoval Gutiérrez: Abogado por la Universidad Santo Tomás, especialista en Derecho Procesal por la Universidad Santo Tomás, especialista en Responsabilidad y Daño Resarcible por la Universidad Externado de Colombia, especialista en Derecho Comercial por la Universidad de los Andes, magíster en Derecho por la Universidad de los Andes. Profesor de la Maestría en Propiedad Intelectual de la Universidad de los Andes. Coordinador del Grupo de Estudios de Derecho de la Competencia y de la Propiedad Intelectual (GEDCOP) de la Universidad de los Andes, miembro del GECTI y del Instituto Colombiano de Derecho Procesal. Durante más de diez años ha trabajado en el ejercicio de facultades jurisdiccionales en procesos de competencia desleal y de infracción de derechos de propiedad industrial.

Dámaso Javier Vicente Blanco: Profesor, doctor e investigador en Derecho Internacional Privado. Premio Extraordinario de Doctorado 2003, poseedor de tres tramos de investigación. Sus publicaciones mantienen una constante en el terreno del análisis de la inversión internacional, de la codificación del derecho internacional privado y el derecho de extranjería en España y en la Unión Europea. Cofundador del "Simposio sobre XML legislativo en España e informática jurídica documental". Vicedecano en la Facultad de Derecho de la Universidad de Valladolid (2004-2010) y director del área de Servicios Jurídicos y Evaluación en el Rectorado de la misma universidad (2010-2012). A la fecha, es director del Departamento de Derecho Mercantil, Derecho del Trabajo y Derecho Internacional Privado de la Universidad de Valladolid.

Derecho de las tecnologías
y las tecnologías para el derecho
se terminó de imprimir
en julio del 2022
en Bogotá, D. C., Colombia