Protección de los datos personales en la era de los algoritmos de la Información

حماية البيانات الشخصية في عصر خوارزميات المعلومات

first researcher: Dr. Bouchra Saidi

Docteur en droit privé

تاريخ الاستلام: 2024/6/21 تاريخ القبول: 2024 /6/24 تاريخ النشر: 2024/7/15

الملخص:

يهدف البحث إلى التعرف أثر اعتماد اللائحة (الاتحاد الأوروبي) 679/2016 وقانون الجمهورية الرقمية مؤخرًا إلى تعزيز – وتوســـيع – حماية البيانات الشخصية. لكن من خلال إرث الأدوات الجديدة التنبؤية، الذي يسمح بإجراء معالجة بدون سوابق من البيانات الرقمية التي يتم إنتاجها من قبل الأفراد، يزرع مفاهيم جديدة في شروط تحويل جميع العمليات، ولكن وسط التمييز والتأثير على الأشخاص. ولذلك، فإن تطبيق الأدوات الآلية لقرارات توما دي يؤدي إلى النظر في طرق تطبيق الأحكام القانونية ويساهم في تغيير تعريف مبدأ البيانات الشخصية.

الكلمات المفتاحية: حماية، البيانات الشخصية، خوارزميات المعلومات.

Abstract

La recherche vise à identifier l'impact La reciente adopción del Reglamento (UE) 2016/679 y la Ley de la República Digital han reforzado –y ampliado– el alcance de la protección de los datos personales. Pero la llegada de nuevas herramientas algorítmicas predictivas, al permitir un procesamiento sin precedentes de rastros digitales producidos por individuos, plantea nuevos riesgos en términos de trazabilidad del procesamiento de datos, pero también de discriminación e influencia en las personas. Por lo tanto, la aplicación de tales herramientas automatizadas de toma de decisiones conduce a cuestionar los métodos de aplicación de las disposiciones legales y contribuye a alterar la definición misma de datos personales.

Keywords: Protection, données personnelles, algorithmes d'information.

Introduction:

La reciente adopción a nivel europeo del Reglamento Europeo de protección de datos personales 2 y, a nivel nacional, la promulgación de la ley para una República Digital 3, han confirmado la importancia de un mayor control sobre los procesos de tratamiento automatizado implementados para capturar, manipular y utilizar datos personales[1]. La protección de estos datos tan específicos, un derecho fundamental consagrado en el artículo 16 del Tratado de Funcionamiento de la Unión Europea y en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, es de hecho necesaria, si no urgente, ante la evolución de las formas en que las personas interactúan con las herramientas digitales conectadas. Sin embargo, en el centro de este cambio, las nuevas formas de toma de decisiones automatizadas han permitido recientemente procesar datos masivos, datos brutos, heterogéneos, dinámicos, característicos del Big Data. Aunque el Big Data no se trata solo de datos personales[2]

y que la gran mayoría de los rastros producidos por los individuos, directamente (ya sea un "clic" en un enlace de Internet, un "me gusta" en una red social) o indirectamente (en forma de metadatos) no constituyen, individualmente, señales de identificación, es evidente que las capacidades de correlación de los procesos de análisis estadístico ya están introduciendo un conjunto fragmentado de datos en el espacio de los datos personales, aparentemente inocuos, que antes estaban excluidos.

Por lo tanto, estos nuevos objetos algorítmicos plantean problemas en la interpretación y aplicación de las disposiciones legales para la protección de datos personales. Capaces de detectar las correlaciones más tenues en los datos producidos por los usuarios de la red, contribuyen a trastocar la definición misma de datos personales, ya sea en términos de información susceptible de identificar a un individuo, ya sea si se trata de reconocer lo que es Ciertas características consideradas sensibles, como el origen étnico, las opiniones políticas o religiosas o los datos relativos a la salud de estas personas. Las sucesivas transformaciones de los datos brutos en datos significativos, dentro de modelos estadísticos opacos, hacen que las disposiciones relativas al deber de explicar el proceso de tratamiento y la trazabilidad de los datos sean en gran medida ineficaces.

---

[1] − Règlement (UE) 2016/679, signé le 27 avril 2016 et publié le 4 mai au Journal officiel de l'Union européenne.

[2] − Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, publiée au Journal officiel le 8 octobre 2016.

Después de describir las características específicas de los algoritmos de aprendizaje, motor del tratamiento de datos masivos, mostraremos cómo la ampliación del campo de interpretación de la noción de datos personales que imponen nos obliga a repensar el equilibrio entre la protección de los derechos fundamentales y la libre circulación de datos [3].A continuación, destacaremos el impacto de los modelos predictivos en las modalidades de aplicación del derecho positivo y de las nuevas disposiciones del Reglamento 2016/679 y de la Ley para una República Digital, tanto en términos de bi-and-greet.

Diversas instituciones, empresas e incluso países con un sistema mundial capitalista abierto han enfatizado en prestar atención al tema de la protección de datos debido al despilfarro de información que provoca este gasto desproporcionado y las pérdidas repetidas debido a la competencia digital y de marketing basada en el elemento de proactividad al violar datos e información personal y con el objetivo de aumentar la visibilidad de sus servicios y reducir significativamente sus pérdidas publicitarias, la empresa decidió utilizar una herramienta de análisis de datos algorítmicos [4] capaz de recopilar información sobre posibles compradores y así reorientar y promocionar sus servicios. Online de una manera más estratégica. Gracias a esta herramienta, las empresas y organizaciones registraron un aumento masivo en sus ventas y en la calidad de sus servicios, al tiempo que gastaron un 75% menos en la gestión de anuncios.

Lo anterior ejemplifica una de las maneras como las herramientas algorítmicas de análisis de datos han derivado en beneficios directos tanto para el sector empresarial, como para el consumidor en el contexto de libre mercado. El sector empresarial, como el primer actor, se beneficia al producir, distribuir e invertir con mayor estabilidad presupuestal, aumentando así su rendimiento económico. El segundo actor, se beneficia al adquirir productos conforme a sus intereses con base en sus búsquedas en la red, aumentando así su grado de satisfacción.[5].Si bien, se destacan los beneficios de este tipo de herramientas, también es importante destacar los límites constitucionales, legales y

[3] – Selon l'article 4 §1 du Règlement (UE) 2016/679, il s'agit là de « *toute information se rapportant à une personne physique identifiée ou identifiable* ».

[4] – Meglena Kuneva, Commissaire Européen à la consommation, Keynote Speech, Roundtable on Online Data Collection, Targeting and Profilin

[5] – REMOLINA, Nelson. *Tratamiento de Datos Personales: Aproximación internacional y comentarios a la ley 1581 de 2012.* Legis, 2013, 82.

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

jurisprudenciales que se podrían oponer a su aplicación cuando no están debidamente reguladas.

En este sentido cabe preguntarse, ¿existen limitaciones en la aplicación de este tipo de herramientas? Y en caso de que la respuesta sea afirmativa, ¿cuál sería la manera más adecuada de regularlas sin desaprovechar los beneficios que estas ofrecen?. Con el ánimo de responder a estos interrogantes, es necesario revisar brevemente cuáles son los fundamentos normativos con el objetivo de (i) reconocer la importancia del rol mediador del Estado en la regulación del uso de estas nuevas tecnologías evidentemente útiles y (ii) ratificar estos fundamentos en los consumidores, en lo que concierne específicamente a la protección de datos personales y los patrones de hábitos de consumo.

En primer lugar, los fundamentos constitucionales que conforman las leyes para la regulación de la protección de datos se constituyen en el derecho fundamental del *habeas data*, esto es, el derecho de conocer, autorizar, incluir y rectificar la información recopilada sobre una persona[6]. Actualmente, la gestión de datos es un tema de análisis constante, puesto que el derecho de *habeas data* conforme al derecho público puede ser exigido por toda persona ante cualquier entidad pública o privada. El reconocimiento de este derecho en las herramientas algorítmicas implementadas en las nuevas tecnologías, que funcionan a partir de la recopilación de datos personales, ha desencadenado en un aumento de las demandas a los Estados, debido a que no se trata únicamente de la obligación habitual de almacenar correctamente los datos de los usuarios por una de las partes, sino de limitar y en ocasiones restringir el acceso a cierto tipo de información, como aquella que se encuentra en los diferentes motores de búsqueda[7].

En segundo lugar, en referencia al marco jurídico legal sobre la protección de datos personales, existen diversas leyes y decretos. El más relevante en relación con la aplicación de las herramientas algorítmicas es la Ley Estatutaria 1281 de 2012, que es reconocida por definir aspectos centrales como la naturaleza de los datos, el grado de responsabilidad según la cantidad de información almacenada, el tipo de tratamiento de los datos y los riesgos potenciales relacionados con la gestión de la información. Lo anterior, en concordancia con el Decreto Único 1074 de 2015, el cual reglamenta los términos y condiciones bajo los cuales se deben inscribir las

---

[6] – REMOLINA, Nelson ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? *International Law: Revista Colombiana De Derecho Internacional,* 2010, no. 16, 489-524.

[7] – RIESGO, Víctor. Nuevas formas de consumo 3.0. El retorno del sujeto al algoritmo. *Teknokultura Revista De Cultura Digital Y Movimientos Sociales*, 2020, 3-11.

bases de datos, la figura del encargado y responsable de los datos personales y el régimen jurídico aplicable a las bases datos.

En tercer lugar, la jurisprudencia de la Corte Constitucional se ha pronunciado sobre el marco normativo de la protección de datos y su aplicabilidad en diferentes sentencias. Por ejemplo, en la sentencia C – 748 de 2011[Cita 9], la Corte ratificó las excepciones para el acceso a las bases de datos contenidas en la Ley de Protección de Datos Personales, asegurando así la prelación del interés general sobre el individual, además de garantizar la seguridad jurídica. Las excepciones ratificadas por la honorable Corte son: las bases de datos personales, las bases de datos relacionadas con la seguridad, la defensa nacional, las bases de datos que almacenen información de inteligencia, contrainteligencia, las bases de datos de información periodística, editorial y, finalmente, las bases de datos de información financiera, comercial, de censos de población y vivienda,[8] las cuales tienen por fin permitir el acceso a la información contenida en las bases de datos cuando la autoridad competente lo considere necesario para salvaguardar el interés general.

En consideración con la excepción de las bases de datos financieras, por ejemplo, en el caso de Datacrédito en Colombia, las centrales de riesgos gestionan la información de los historiales crediticios de los consumidores sin tomar decisiones directamente sobre los datos que recopilan, pero haciendo un análisis general sobre el estado financiero de los consumidores en el país por medio de los datos recopilados en las bases de datos. Sin embargo, recientemente esta información ha sido analizada mediante plataformas algorítmicas, con el objetivo de asignar puntajes de riesgo a los consumidores financieros[9]. Lo anterior vulnera los pilares constitucionales y económicos, tales como la democratización del crédito o la garantía de un mínimo vital. No obstante, se permite el acceso a dicha información como una de las excepciones de las bases de datos financieras, ya que representa un beneficio directo para el sector bancario, financiero y comercial.

---

[8] – SIC (Superintendencia de Industria y Comercio). *Guía para la implementación del principio de responsabilidad demostrada en las trasferencias internacionales de datos personales*. Delegatura para la protección de datos personales, 2019, 9–12.

[9] – Los tipos de datos principalmente son: públicos, semiprivado, privado y sensible, según el grado de protección y sensibilidad. REMOLINA, Nelson ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? *International Law: Revista Colombiana De Derecho Internacional,* 2010.

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

En virtud de lo anterior, surge otro interrogante. ¿Qué sucede si un empresario decide usar una herramienta algorítmica de recopilación de datos para publicitar un servicio dirigido a un tipo específico de consumidor como lo hizo la empresa RedBalloon en Australia o incluso, publicitar usando la algoritmia de las redes sociales como Facebook, Twitter o Instagram?, ¿estaría sujeto a algún tipo de responsabilidad jurídica?. La respuesta en principio, a pesar de ciertos desafíos y bajo ciertas condiciones, es que no lo está.

El grado de responsabilidad sobre el manejo de los datos está contenido en los fundamentos legales y en las directrices internacionales,[10] las cuales varían de acuerdo al tipo,[11]. y la cantidad de información que almacene y gestione una organización. De esta forma, una multinacional capaz de almacenar información de millones de personas tendría una responsabilidad proporcionalmente más alta frente a los Estados y las autoridades internacionales en comparación con una microempresa que usa información de herramientas algorítmicas para promocionar un producto en línea o una empresa que la usa para aumentar sus ventas. Ahora bien, sin perjuicio del grado de responsabilidad de las empresas grandes o pequeñas, ambas situaciones pueden tener potencialmente un resultado negativo en los consumidores y en la dismininución de los hábitos de consumo, cuando emerge en los consumidores una sensación de invasión del espacio personal y de la privacidad generando un sentimiento de aversión hacia determinado producto.

En relación a este último punto, el mayor impacto del uso de la algoritmia de la información en los mercados ha sido la trasformación de los consumidores en meros proveedores de dato que proveen estadísticas económicas, y que maximizan la ganancias de una empresa, ignorando, en muchas ocasiones, el bienestar de los consumidores y la consolidación de hábitos de consumos responsables que impliquen el cuidado de los recursos y el manejo adecuado de la información.[12]

Entonces, si una empresa paga a una red social con la intención de publicitar sus productos a consumidores potenciales y tener provecho de la información que almacena, en esencia, no incurriría en el mismo grado de responsabilidad que la organización prestadora de este tipo de servicios[13], puesto que la red social tendría un mayor grado de responsabilidad sobre el uso de los datos que recopila. Sin

[10] URUEÑA, René. Autoridad algorítmica: ¿cómo empezar a pensar la protección de los derechos humanos en la era del 'big data'? *Latin American Law Review* no. 02, 2019, 99-124

[11] – Corte Constitucional, sentencia C – 1011 de 2008, M.P. Jaime Córdoba Triviño

[12] – Corte Constitucional, sentencia C – 748 de 2011, M.P. Jorge Ignacio Pretel.

[13] – Corte Constitucional, sentencia T – 176A de 2014 M.P. Jorge Ignacio Pretelt

embargo, el grado de responsabilidad depende del tipo de información, la forma de gestionarla, su uso y, adicionalmente, el análisis de cada caso en particular.

En Colombia, por ejemplo, se prohíbe en cualquier circunstancia "la transferencia de datos personales de cualquier tipo a países que no propicien niveles adecuados a la protección de datos".[14] En este sentido, toda organización nacional e internacional debe respetar los estándares regulatorios nacionales sobre la protección de los datos personales y para ello se han fijado acciones administrativas[15], que propicien una protección total y no parcial. A pesar de esto, el marco regulatorio colombiano en términos generales no constituye un tipo de responsabilidad especial al sector empresarial en estas situaciones.

En consecuencia, ¿será esta la manera más adecuada de regular y aprovechar los beneficios de este tipo de herramientas tecnológicas?. La investigación sobre nuevas tecnologías y su aplicabilidad en el derecho de cada Estado resulta, en definitiva, intrincada en ciertos aspectos. El principal inconveniente es que el ordenamiento jurídico que pretende regular las innovaciones tecnológicas no avanza a la misma velocidad que la tecnología. Sin embargo, una normatividad que se fundamente en principios como los contenidos en la Constitución, en los instrumentos internacionales y en la legislación de protección de datos personales, brindan las herramientas esenciales para comprender nuevos casos de estudio de tecnologías que innoven o que estén en constante evolución como, por ejemplo, las herramientas algorítmicas en relación a la protección de datos personales.

En suma, la regulación actual es pertinente en definir los principios que eventualmente se convertirán en criterios interpretativos y reglamentos que lograrán adaptarse a las innovaciones tecnológicas en constante evolución. Entre estos principios se incluyen los contenidos en las leyes estatutarias, los decretos, la jurisprudencia y la doctrina. Algunos de estos son: libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida de la información y los principios de diligencia y seguridad[16]. Ahora bien, una cuestión a tener en cuenta para investigaciones futuras es si la regulación actual no puede

---

[14]– La herramienta algorítmica a la que se hace referencia en este caso es conocida como "Albert" una plataforma digital encargada de recopilar información y gestionar anuncios en líne

[15] – RIESGO, Víctor. Nuevas formas de consumo 3.0. El retorno del sujeto al algoritmo. *Teknokultura Revista De Cultura Digital Y Movimientos Sociales,* 2020, 3-11.

[16] – CORTE CONSTITUCIONAL, sentencia T-176A de 2014, M.P. Jorge Ignacio Pretelt. Esta sentencia trata los fundamentos del derecho al buen nombre y al *habeas data*.

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

abordar en su totalidad los problemas jurídicos derivados de la complejidad de los avances tecnológicos ¿será necesario establecer una regulación normativa especial por medio de un consenso entre los desarrolladores tecnológicos, el Estado y la sociedad?

Las leyes y normativas españolas, especialmente el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos (LOPD), juegan un papel importante para garantizar el uso responsable de los datos personales en la toma de decisiones algorítmicas. Estos marcos establecen directrices claras para la protección de datos, la transparencia y los derechos individuales.

fecha a partir de la cual será directamente aplicable en todos los Estados miembros de la Unión Europea 54.

El derecho a la protección de los datos personales, tal como se establece en estos textos, tiene por objeto garantizar el respeto de los derechos y libertades fundamentales. 55 El Convenio 108 enfatizó hace más de 35 años que "en ciertas condiciones, el ejercicio de la plena libertad para procesar la información puede perjudicar el disfrute de otros derechos fundamentales (por ejemplo, los derechos a la privacidad, a la no discriminación y a un juicio justo) u otros intereses personales legítimos (por ejemplo, en relación con el empleo o el crédito al consumo). Con el fin de mantener un justo equilibrio entre los diferentes derechos e intereses de las personas, la Convención impone ciertas condiciones o restricciones al tratamiento de la información. »

«Debe reforzarse la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas». Por lo tanto, para que sea eficaz, la aplicación de este control debe examinarse a la luz de las especificidades del objeto algorítmico al que se aplica. Este examen crítico debe llevarse a cabo tanto desde el punto de vista técnico [17]como desde el punto de vista jurídico [18]y debe conducir a un replanteamiento de los medios de protección de los datos personales [19].

---

[17] – T. Calders, Toon et I. Žliobaitė. Why unbiased computational processes can lead to discriminative decision procedures. Discrimination and Privacy in the Information Society. Springer, 2013, p. 43–57.

[18] – S. Barocas et A.D. Selbst. Big data's disparate impact. California Law Review, 2016, vol. 104, p. 671–731.

[19] – Para un resumen de los cambios introducidos por el nuevo reglamento, véase C. C. Castets-Renard, Breve análisis del Reglamento General de protección de datos personales. Dalloz IP/IT, julio de 2016, p. 334. Otros textos comunitarios también se refieren a la protección de los datos

Normas y principios clave

Oficial de Protección de Datos: Las organizaciones deben designar un Oficial de Protección de Datos para supervisar el cumplimiento de las leyes de protección de datos (Blanco, 2018).

Requisitos de transparencia: El RGPD establece que los interesados reciben información útil sobre la lógica implicada en las decisiones automatizadas, lo que mejora la transparencia en los procesos algorítmicos (Brkan, 2019) (Brkan, 2018).

Derechos de las personas físicas: Los usuarios pueden ejercer derechos como la supresión, restricción y portabilidad de los datos, y reforzar su control sobre los datos personales (Blanco, 2018).

Contexto laboral:

Derechos de los consejos de trabajadores: Las recientes reformas en España exigen a los empleadores que descubran normas de toma de decisiones algorítmicas para los consejos de trabajadores, y que refuercen la gobernanza colectiva y la rendición de cuentas en las aplicaciones de IA en el lugar de trabajo (Durán, 2023).

personales: en particular, el Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, adoptado por el Consejo de Europa el 28 de enero de 1981, pero también la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, de 12 de julio de 2002, modificada por la Directiva 2006/24/CE, de 15 de marzo de 2006, relativa a la conservación de datos.

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

Sources et références:

CORTE CONSTITUCIONAL, sentencia T-176A de 2014, M.P. Jorge Ignacio Pretelt. Esta sentencia trata los fundamentos del derecho al buen nombre y al *habeas data*.

La herramienta algorítmica a la que se hace referencia en este caso es conocida como "Albert" una plataforma digital encargada de recopilar información y gestionar anuncios en líne

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, publiée au Journal officiel le 8 octobre 2016**.**

Los tipos de datos principalmente son: públicos, semiprivado, privado y sensible, según el grado de protección y sensibilidad. REMOLINA, Nelson ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? *International Law: Revista Colombiana De Derecho Internacional,* 2010.

Meglena Kuneva, Commissaire Européen à la consommation, Keynote Speech, Roundtable on Online Data Collection, Targeting and Profilin

Para un resumen de los cambios introducidos por el nuevo reglamento, véase C. C. Castets-Renard, Breve análisis del Reglamento General de protección de datos personales. Dalloz IP/IT, julio de 2016, p. 334. Otros textos comunitarios también se refieren a la protección de los datos personales: en particular, el Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, adoptado por el Consejo de Europa el 28 de enero de 1981, pero también la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, de 12 de julio de 2002, modificada por la Directiva 2006/24/CE, de 15 de marzo de 2006, relativa a la conservación de datos.

Règlement (UE) 2016/679, signé le 27 avril 2016 et publié le 4 mai au Journal officiel de l'Union européenne.

REMOLINA, Nelson ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? *International Law: Revista Colombiana De Derecho Internacional,* 2010, no. 16, 489-524.

REMOLINA, Nelson. *Tratamiento de Datos Personales: Aproximación internacional y comentarios a la ley 1581 de 2012.* Legis, 2013, 82.

RIESGO, Víctor. Nuevas formas de consumo 3.0. El retorno del sujeto al algoritmo. *Teknokultura Revista De Cultura Digital Y Movimientos Sociales*, 2020, 3-11.

S. Barocas et A.D. Selbst. Big data's disparate impact. California Law Review, 2016, vol. 104, p. 671-731.

Selon l'article 4 §1 du Règlement (UE) 2016/679, il s'agit là de « *toute information se rapportant à une personne physique identifiée ou identifiable* ».

SIC (Superintendencia de Industria y Comercio). *Guía para la implementación del principio de responsabilidad demostrada en las trasferencias internacionales de datos personales*. Delegatura para la protección de datos personales, 2019, 9-12.

T. Calders, Toon et I. Žliobaitė. Why unbiased computational processes can lead to discriminative decision procedures. Discrimination and Privacy in the Information Society. Springer, 2013, p. 43-57.