La regulación del derecho a la protección de datos en los Estados Unidos: hacia un RGPD norteamericano

The regulation of data protection law in the United States: towards an American GDPR

Moisés Barrio Andrés

Letrado del Consejo de Estado - Doctor en Derecho - Profesor de Derecho Digital Director del Diploma de Alta Especialización en Legal Tech y transformación digital (DAELT) de la Escuela de Práctica Jurídica de la Universidad Complutense de Madrid

Recibido: 01.07.2022 / Aceptado: 19.07.20220
DOI: 10.20318/cdt.2022.7181

Resumen: Este estudio aborda el examen de los marcos jurídicos existentes en materia de privacidad y protección de datos en los Estados Unidos, tanto a nivel federal como estatal. Constituyen un intrincado puzle regulatorio que ha sido duramente criticado por su falta de eficacia, obsolescencia y deficiente técnica normativa. Los Estados, por su parte, han comenzado a promulgar sus respectivas leyes tuitivas, lo cual crea diferentes obligaciones para las empresas sin garantizar de forma coherente que los individuos reciban una protección adecuada. Esta situación aspira ser corregida por medio de una próxima ley federal en la materia: la *American Data Privacy and Protection Act* (ADPPA), cuyas líneas maestras se exponen en el trabajo.

Palabras clave: American Data Privacy and Protection Act (ADPPA); privacidad; protección de datos.

Abstract: This paper addresses the review of the existing privacy and data protection legal frameworks in the United States, both at the federal and state levels. They constitute an intricate regulatory puzzle that has been heavily criticized for its lack of effectiveness, obsolescence, and poor regulatory technique. The States, for their part, have begun to enact their respective privacy and data protection laws, which create different obligations for companies without consistently ensuring that individuals receive adequate protection. This situation is expected to be corrected by means of a forthcoming federal law on the subject: the American Data Privacy and Protection Act (ADPPA), the outlines of which are set out in the paper.

Keywords: American Data Privacy and Protection Act (ADPPA); privacy; data protection.

I. Introducción

1. En los Estados Unidos, y a pesar de lo que pudiera parecer, la mayor parte de los marcos jurídicos existentes en materia de privacidad y protección de datos, tanto a nivel federal como estatal, ofrecen salvaguardias incompletas contra bastantes de los atentados y daños a la privacidad y la seguri-

dad de la información que se vienen produciendo desde la generalización[1] de Internet. Muchos de estos grupos normativos han sido criticados durante largo tiempo por los expertos[2] en derecho de la privacidad, quienes subrayan su falta de eficacia, obsolescencia y deficiente técnica normativa. Ahora, las tecnologías disruptivas como la robótica, la inteligencia artificial, *blockchain*, el Internet de las Cosas o el metaverso, amplían exponencialmente estas deficiencias, ya que agravan los problemas de privacidad y protección de datos existentes.

2. En efecto, por el momento no existe una única ley federal que regule de forma exhaustiva el uso de los datos personales de los ciudadanos. Aunque se reconoce un derecho constitucional a la privacidad individual amparado por el Tribunal Supremo, en esencia este derecho protege a la persona contra la intrusión del poder público, pero hace "poco para evitar que los actores privados abusen de los datos personales en línea", tal y como denunció hace mucho tiempo el profesor FROOMKIN.[3] Además, el marco normativo federal vigente carece de uniformidad, tal y como tendremos ocasión de comprobar en el próximo epígrafe. A ello se suma la competencia concurrente de varias agencias federales para hacer cumplir la amplia gama de leyes y reglamentos de privacidad y protección de datos en este escalón federal.

3. En cuanto al nivel estatal, a fecha de escribir estas líneas en junio de 2022 cinco Estados ya han promulgado sus respectivas leyes tuitivas, y más de la mitad de los Estados están desarrollando iniciativas legislativas al respecto. Pero este mosaico de normas crea diferentes obligaciones para las empresas sin garantizar de forma coherente que los individuos reciban una protección adecuada. Incluso, la pionera *California Consumer Privacy Act* de 2018, la CCPA, tiene varias limitaciones y lagunas[4], y por eso ha tenido que ser reformada en 2020, como señalaremos más adelante. A examinar estos dos niveles de legislación, federal y estatal, dirigiremos nuestros próximos pasos.

II. La regulación federal de la protección de datos

4. La apuntada ausencia de una ley principal federal en la materia ha venido siendo suplida por medio de un acervo de leyes y reglamentos federales sobre privacidad que varían en cuanto a su finalidad y alcance. Los podemos ordenar en dos grupos. Un primer conjunto de estas leyes se caracteriza por el tipo específico de información que pretende regular. Por ejemplo, la *Cable Communications Privacy Act* de 1984 regula la privacidad de la información de los servicios de telecomunicaciones por cable.[5] Otras leyes notables sobre privacidad de los datos en este grupo son la *Computer Fraud and Abuse Act* de 1986[6], la *Video Privacy Protection Act* de 1988[7] y la *Children's Online Privacy Protection Act* (COPPA) de 1998[8], concernientes, respectivamente, a los datos obrantes en un sistema informático, a los de alquiler o venta de material audiovisual y a los datos de los menores de edad.

5. El segundo conjunto normativo se contiene en la legislación federal sectorial. Los cuatro ámbitos principales con regulación propia en la materia son los servicios financieros, la sanidad, las telecomunicaciones y la educación. En el sector de los servicios financieros, la *Fair Credit Reporting Act* de 1970, modificada posteriormente por la *Fair and Accurate Credit Transactions Act* de 2003[9], regula el uso de la información personal relacionada con el crédito. Además, la *Gramm-Leach-Bliley Act*

[1] Lo hemos estudiado detenidamente en M. Barrio Andrés, *Fundamentos del Derecho de Internet*, Madrid, Centro de Estudios Políticos y Constitucionales, 2.ª edición, 2020, pág. 74 y ss.

[2] Por ejemplo, D. J. Bodenhamer (ed.), *The Bill of Rights in modern America*, Bloomington (Indiana), Indiana University Press, 2022, 3.ª edición, capítulo 9.

[3] A. M. Froomkin, "The Death of Privacy?", *Stanford Law Review*, Vol. 52, 2000.

[4] S. W. Pink, *California Consumer Privacy Act Annotated*, California, Practising Law Institute (PLI), 2020, §1.1.22.

[5] 47 U.S.C. § 551(a)–(h).

[6] 18 U.S.C. § 1030 (Supp. II 1987).

[7] 18 U.S.C. § 2710.

[8] 15 U.S.C. §§ 6501–6506.

[9] 15 U.S.C. §§ 1681–1681x.

(GLBA) de 1999[10] disciplina el uso de los datos personales que están en manos de entidades de servicios financieros, como los bancos y las aseguradoras. La GLBA tutela el uso de la "información personal no pública", que incluye la información personal que las empresas de servicios financieros recogen[11] en relación con sus productos o servicios.

6. En cuanto a los datos relativos a la salud, la ley federal más importante en materia de privacidad y protección de estos datos es la *Health Information Portability and Accountability Act* (HIPAA) de 1996.[12] Esta ley rige el uso y la privacidad de la información sanitaria que poseen las entidades objeto de la norma, como los hospitales u otros proveedores de servicios médicos. Además, impone requisitos de ciberseguridad que protegen la información sanitaria personal. La HIPAA restringe la capacidad de los sujetos obligados de intercambiar, vender o divulgar los datos protegidos, salvo que medie consentimiento del interesado. De forma similar a la HIPAA, la *Family Educational Rights and Privacy Act* (FERPA) de 1974[13] reconoce el derecho de los estudiantes y sus familias a acceder a sus registros educativos, incluida la información personal sobre el estudiante, y a prohibir la divulgación de los registros sin consentimiento. Pero la FERPA sólo tutela los registros personales en el sector educativo, dejando muchos datos sin protección. Por ejemplo, una grabación de vídeo de una clase en línea sólo constituye un registro educativo[14] bajo la FERPA si "son directamente concernientes a un estudiante y son mantenidos por una institución educativa". Por último, la *Telephone Consumer Protection Act* de 1991[15] disciplina la ejecución de las llamadas y los mensajes de texto automáticos de contenido publicitario a los consumidores.

7. Para concluir la exposición general de las leyes federales de privacidad actuales, debemos notar que varias agencias administrativas tienen jurisdicción para hacer cumplir el complicado puzle normativo. Sin embargo, Estados Unidos no cuenta con una agencia reguladora exclusiva para la protección de datos y la privacidad. Como ya sabemos, las leyes son específicas del sector o correspondientes a la concreta naturaleza de la información y son aplicadas por diferentes agencias federales, a menudo con competencias no bien delimitadas. Algunas de estas agencias son el Departamento de Comercio del Gobierno Federal (DoC por sus siglas inglesas), la Comisión de Valores y Bolsa (SEC), la Comisión Federal de Comunicaciones (FCC) y el Departamento de Salud y Servicios Humanos (HHS). De estas, las dos agencias con las potestades más amplias para la aplicación de la regulación de la protección de datos personales son la Comisión Federal de Comercio (la FTC o Federal Trade Commission) y la Oficina de Protección Financiera del Consumidor (la CFPB o Consumer Financial Protection Bureau).

8. Más específicamente, la FTC ostenta la más amplia jurisdicción y autoridad sobre la privacidad de los datos, cubriendo efectivamente los vacíos regulatorios dejados por otras normas federales, tal y como han estudiado HARTZOG y SOLOVE.[16] Su autoridad se deriva de la sección quinta de la *Federal Trade Commission Act* (FTCA) de 1914, que prohíbe los "actos o prácticas desleales o engañosos" que afecten al comercio.[17] La sección quinta de la Ley define el alcance de la cláusula de "actos o prácticas desleales o engañosos" (es decir, los *unfair and deceptive acts or practices* o UDAP) en relación con el comercio dentro de naciones extranjeras.[18] La sección quinta faculta a la FTC a proteger a los consumidores contra los UDAP investigando e iniciando acciones contra las empresas que actúan de forma engañosa o desleal. En el ámbito de la protección de datos, la FTC afirma que "las empresas actúan de forma engañosa cuando recopilan, utilizan o revelan información personal de una manera

[10] 15 U.S.C. §§ 6801–6809, 6821–6827.
[11] *Ex* 15 U.S.C. § 6809(9).
[12] Public Law No. 104-191, 110 Stat. 1936.
[13] 20 U.S.C. § 1232g.
[14] 20 U.S.C. § 1232g(a)(5).
[15] 47 U.S.C. § 227.
[16] W. Hartzog y D. J. Solove, "The Scope and Potential of FTC Data Protection", *George Washington Law Review*, Vol. 83, 2015.
[17] 15 U.S.C. § 45(a)(1).
[18] 15 U.S.C. § 45(a)(1).

que contradice su política de privacidad publicada u otras declaraciones, o cuando no protegen adecuadamente la información personal".[19] Ahora bien, sus potestades están limitadas por lo establecido en la FTCA. Por ejemplo, en la mayoría de los asuntos concernientes a la protección de datos, la FTC no puede imponer sanciones civiles. Por eso, la FTC ha venido promoviendo una autorregulación en la materia, preocupada también por la posible afectación que la regulación pudiera tener en la innovación.

9. De forma similar a la competencia de la FTC sobre los UDAP, la CFPB tiene jurisdicción para abordar los actos o prácticas desleales o engañosos, así como las prácticas "abusivas" en el sector financiero.[20] La CFPB reputa que un acto o práctica es abusivo si "interfiere materialmente con la capacidad de un consumidor para entender un término o condición de un producto o servicio financiero de consumo"[21], o si se aprovecha de forma irrazonable de la falta de comprensión del consumidor o de su incapacidad para proteger sus intereses. En la actualidad, la CFPB sólo tiene jurisdicción en el contexto de los servicios y productos financieros. La señalada Oficina de Protección Financiera del Consumidor se ha mostrado reacia a ampliar su competencia más allá de esos límites en el espacio más amplio de la privacidad y la seguridad de los datos, al decir de VAN LOO.[22]

10. A la postre, y debido a que no existe una ley federal completa en este campo, hay cientos de requisitos legales dispares relacionados con los datos de los ciudadanos y la privacidad, según ha estudiado TRAUTMAN.[23] La falta de uniformidad regulatoria complica el cumplimiento normativo y la seguridad jurídica, y deja a los consumidores sin un entendimiento real de sus derechos sobre los datos personales.

11. Como botón de muestra, podemos traer a colación el uso de datos de salud. Muchos ciudadanos revelan en línea información detallada y sensible sobre su salud. A través de tecnocomplementos o *werables*, publicaciones en las redes sociales, búsquedas en la Web y las interacciones en foros de pacientes en línea, los usuarios generan grandes volúmenes de datos de salud, lo cual se agrava de forma paradigmática en el Internet de las Cosas.[24] Sin embargo, la HIPAA sólo obliga a las entidades enumeradas en el ámbito de aplicación de la norma que "poseen información sanitaria protegida", y únicamente cubre los datos sanitarios identificables. De este modo, servicios de la sociedad de la información como los que prestan Google, Facebook y Twitter no quedan comprendidos en el ámbito de aplicación de la HIPAA. Tampoco quedan cubiertos los dispositivos del IoT, porque "no proporcionan servicios médicos o de salud".[25] Asimismo, los datos de salud anonimizados no están protegidos por dicha ley. De este modo, y como advierte DETERMANN, las empresas pueden "utilizar los datos de salud para diversos fines dirigidos a los consumidores y a los pacientes sobre la base de perfiles elaborados a partir del comportamiento de los usuarios rastreados, los datos adquiridos de otras fuentes y los análisis predictivos".[26] Las importantes lagunas e incoherencias normativas en materia de privacidad de los datos de salud son sólo un ejemplo de cómo el actual esquema normativo no favorece la supervisión eficaz ni la salvaguardia de los datos personales.

III. La regulación estatal de la protección de datos

12. A nivel de los Estados cabe detectar en esta década una honda preocupación por la protección de datos y su efectiva regulación. Unas dos docenas de Estados han propuesto su propia legislación, han

[19] https://www.ftc.gov/about-ftc/mission
[20] 12 U.S.C. § 5531(d).
[21] *Ídem*.
[22] R. Van loo, "Rise of the Digital Regulator", *Duke Law Journal*, Vol. 66, 2017, pág. 1310.
[23] L. J. Trautman, "Governance of the Facebook Privacy Crisis", *Pittsburgh Journal of Technology Law & Policy*, Vol. 20, 2020.
[24] M. Barrio Andrés, *Internet de las Cosas*, Madrid, Editorial Reus, 3.ª edición, 2022, pág. 58.
[25] 42 U.S.C. § 17935(d).
[26] L. Determann, "Healthy Data Protection", *Michigan Telecommunications and Technology Law Review*, Vol. 26, 2020, pág. 229.

designado grupos de trabajo o ya han promulgado leyes estatales de protección de datos en los últimos años. El hilo conductor ha sido la protección de los consumidores, como subraya SCHWARTZ.[27] Las normas estatales introducen un tímido conjunto de derechos y obligaciones en la materia, en comparación con el elevado estándar europeo[28] constituido por el Reglamento General de Protección de Datos.[29] En cuanto a las obligaciones que se imponen a los responsables del tratamiento, algunas normas exigen la notificación de las violaciones de seguridad de los datos, la evaluación de impacto de la protección de datos, la aceptación expresa de la venta de datos y un requisito de transparencia. Por lo que se refiere a los derechos de los ciudadanos, se reconocen los tradicionales derechos ARCO (acceso, rectificación, cancelación y oposición), a través de los cuales los ciudadanos pueden conocer en todo momento quién dispone de sus datos y para qué fines están siendo utilizados.

13. En junio de 2022, cinco Estados ya han promulgado con éxito leyes de privacidad estatales completas que regulan la protección de los datos de los consumidores: California[30], Virginia[31] y, más recientemente, Colorado[32], Utah[33] y Connecticut.[34] Por su parte, Illinois[35] ha implementado una ley de privacidad de datos biométricos.

14. La pionera *California Consumer Privacy Act* (CCPA, por sus siglas en inglés) de 2018 entró en vigor en 2020 y ya ha tenido un impacto nacional. Si bien su ámbito de aplicación está limitado *ex lege* al estado californiano, pues protege a las personas físicas residentes en el mismo, la importancia de las empresas afectadas por la norma, que incluye a gigantes de Internet como Google, Facebook, Amazon y Microsoft, la dota, en la práctica, de una eficacia nacional. La Ley, que ha sido ampliada por medio de la *California Privacy Rights Act* (CPRA) de 2020[36] –tanto en nuevos derechos como con la creación de una agencia estatal de protección de datos[37]–, está sirviendo de modelo normativo de muchos Estados.

15. La CCPA confiere a los consumidores tres derechos principales: en primer lugar, los residentes en California tienen derecho a conocer la información que las empresas han recopilado de ellos y si las empresas han vendido esta información; en segundo lugar, tienen derecho a optar por la venta de su información personal recopilada; y, por último, los allí residentes tienen derecho a eliminar sus datos personales recogidos, en determinadas circunstancias. La reforma de 2020 por medio de la CPRA limita la posibilidad de intercambio de datos personales, así como de datos personales sensibles, e introduce el derecho a la exactitud de los datos en cuya virtud los consumidores podrán exigir a las empresas que traten sus datos que realicen esfuerzos razonables para corregir los datos personales que poseen.

IV. Hacia una ley federal de protección de datos: la *American Data Privacy and Protection Act* (ADPPA)

16. Ya en septiembre de 2018, la Administración Nacional de Telecomunicaciones e Información (National Telecommunications and Information Administration o NTIA) del Departamento federal

[27] P. M. Schwartz y D. J. Solove, *Privacy Law Fundamentals*, Nueva York, IAPP, 6.ª edición, 2022, capítulo 1.

[28] M. Barrio Andrés, *Manual de Derecho digital*, Valencia, Editorial Tirant lo Blanch, 2.ª edición, 2022, pág. 257 y ss.

[29] Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos o RGPD en lo sucesivo).

[30] California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–1798.199 (West 2018).

[31] Virginia Consumer Data Protection Act, Va. Code Ann. §§ 59.1-575 al 59.1-585.

[32] Colorado Privacy Act, Colo. Rev. Stat. Ann. §§ 6-1-1301 al 6-1-1313 (West 2021).

[33] Utah Consumer Privacy Act, S.B. 227.

[34] Connecticut Data Privacy Act. Public Act No. 22-15.

[35] Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1 (2008).

[36] Cal. Civ. Code § 1798.100, *et seq*.

[37] La California Privacy Protection Agency (CPPA).

de Comercio abrió una consulta pública previa titulada "*Developing the Administration's Approach to Consumer Privacy*".[38]

17. El objetivo de la consulta era determinar cómo proteger mejor la privacidad de los consumidores y, al mismo tiempo, fomentar la innovación. El texto de la consulta ponía de manifiesto los cambios derivados del entorno digital, "incluida la omnipresencia de la recopilación de datos personales", y señalaba que los usuarios tienen una creciente preocupación por la privacidad de su información personal en línea. También ilustró cómo las actuales regulaciones federales fragmentadas desincentivan la innovación y dificultan el cumplimiento normativo para muchas empresas. El documento de la consulta esbozó el enfoque general de la Administración Trump para regular la privacidad de los consumidores: promulgar una regulación federal que aumente los resultados tuitivos de la privacidad de los consumidores y que, al mismo tiempo, auspicie un ecosistema regulatorio que permita un cumplimiento más fácil para mejorar la competencia y la innovación. La consulta proponía que fuera la FTC la agencia federal apropiada para hacer cumplir las regulaciones de protección de datos de los consumidores, a pesar de reconocer su falta de jurisdicción sobre otras leyes de privacidad como la HIPAA. Finalizada la consulta, con fecha 13 de noviembre de 2018, la NTIA comunicó[39] que había recibido más de 200 comentarios en respuesta a la consulta por parte de individuos, asociaciones de la industria, empresas, sociedad civil y académicos. También publicó[40] todas las observaciones recibidas.

18. Aunque la Administración Biden aún no ha dado a conocer un plan concreto para la legislación federal sobre protección de datos, su Administración ha adoptado algunas medidas relacionadas con la materia. En particular, nuevamente la NTIA, ahora bajo la Administración Biden, ha organizado tres audiencias públicas relativas a los datos personales en diciembre de 2021, específicamente sobre la intersección de la privacidad, la equidad y los derechos civiles.[41] El presidente Biden también expidió una Orden Ejecutiva en julio de 2021 y titulada "*Promover la competencia en la economía estadounidense*", con posibles implicaciones para la tutela de la privacidad y la supervisión, que quedó encomendada a la FTC, de la acumulación de grandes cantidades de datos.[42]

19. De forma paralela, casi la mitad de los Estados están preparados para aprobar sus propias leyes de protección de datos en los próximos años, lo que agravará aún más las incoherencias en la regulación de esta materia en aquel país, como bien ha señalado un prestigioso sector doctrinal.[43] Los factores internacionales también pueden animar a la Administración Biden a impulsar una regulación integral de la protección de datos. La Unión Europea y Estados Unidos siguen negociando después de que el Tribunal de Justicia de la Unión Europea anulara de nuevo el acuerdo de intercambio de datos entre la UE y Estados Unidos, conocido como el *Data Privacy Shield*, el pasado 16 de julio de 2020.[44] A mi juicio, una solución factible al problema de las transferencias internacionales de datos entre ambos sujetos de Derecho Público sería promulgar allí una ley federal de privacidad de datos uniforme.

20. La situación puede cambiar si finalmente se aprueba la llamada *American Data Privacy and Protection Act* (ADPPA), que fue presentada con fecha 3 de junio de 2022[45] por un grupo de congresistas y senadores norteamericanos, de ambos partidos. Este proyecto de ley es la primera propuesta global de privacidad que obtiene un apoyo bipartidista y bicameral en Estados Unidos, y representa la mejor

[38] https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy

[39] https://www.ntia.doc.gov/press-release/2018/ntia-releases-comments-proposed-approach-protecting-consumer-privacy

[40] https://www.ntia.doc.gov/other-publication/2018/comments-developing-administration-s-approach-consumer-privacy

[41] https://www.ntia.doc.gov/files/ntia/publications/fr-ntia-listening-sessions-11302021.pdf

[42] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/

[43] P. M. Schwartz y D. J. Solove, *op. cit*., pág. 6.

[44] STJUE de 16 de julio de 2020, *Facebook Ireland y Schrems II*, asunto C-311/18.

[45] H.R. 8152. Disponible en https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf

oportunidad para aprobar un marco federal de privacidad en décadas. La futura norma protegerá la privacidad y la seguridad de los datos de los consumidores e impedirá que las empresas recopilen éstos en exceso y hagan un uso indebido de los datos de los ciudadanos estadounidenses, a la vez que tutelará a los menores, empoderará a los consumidores y proporcionará sólidos mecanismos de aplicación. Se trata de una norma profundamente inspirada en el RGPD. Su supervisión correrá a cargo de una sección especializada de la FTC, desechando el proyecto de ley la opción en favor de una nueva agencia independiente *ad hoc*.

21. Los datos incluidos en el ámbito de aplicación del proyecto de ley (los *covered data*), se definen como "información que identifica o está vinculada o razonablemente vinculada a una persona o a un dispositivo que identifica o está vinculado o razonablemente vinculado a una o más personas, incluidos los datos derivados y los identificadores únicos". En cambio, no quedan comprendidos los datos anonimizados (*de-identified data*), los datos de los empleados o la información disponible públicamente. La FTC se encargará de emitir próximas orientaciones adicionales en las que precisará el alcance de estos conceptos.

22. El proyecto de ley impone a todas las entidades que traten datos personales cubiertos por la norma la obligación de no recopilar ni utilizar innecesariamente dichos datos, es decir, el principio de minimización de datos. Los sujetos obligados tendrán la obligación de aplicar políticas, prácticas y procedimientos razonables para recoger, procesar y transferir los datos cubiertos. Además, los sujetos obligados tendrán que proporcionar a los individuos políticas de privacidad que detallen las actividades de tratamiento, transferencia y seguridad de los datos de una manera fácilmente disponible y comprensible. Las políticas deberán incluir información de contacto, las filiales de la entidad cubierta a las que se transfieren los datos cubiertos, y los fines de cada categoría de datos cubiertos que el responsable del tratamiento recoge, procesa y transfiere.

23. Por otra parte, los sujetos obligados tendrán prohibido condicionar de forma directa o indirecta la prestación o terminación de servicios o productos a los interesados haciendo que éstos renuncien a cualquier derecho establecido por la futura ley. También se prevé una responsabilidad ejecutiva adicional para los grandes titulares de datos, incluyendo la exigencia de que los CEO y los responsables de privacidad certifiquen anualmente que su empresa mantiene controles internos razonables y estructuras de información para el cumplimiento de la norma.

24. Una novedad de calado es el establecimiento de un conjunto de derechos de los ciudadanos. Se reconocen así los derechos de las personas a acceder, rectificar, suprimir y transferir los datos cubiertos que les conciernen. Estos derechos son similares a muchos de los que disfrutan los residentes de California en virtud de la CCPA de 2018. El derecho de acceso incluiría la obtención de los datos cubiertos en un formato legible y descargable de forma gratuita, así como que los individuos puedan conocer a quienes se han transferido los datos, las categorías de fuentes utilizadas para recoger cualquier dato cubierto y los fines del tratamiento y transferencias de los datos. Los derechos de rectificación y supresión de los datos implican el deber de las entidades afectadas de notificar a otras entidades a las que se transfirieron los datos la información corregida o la voluntad de que se eliminen los mismos.

25. Para cerrar el examen de las novedades más relevantes, debemos referirnos a la regulación de los algoritmos. Los sujetos obligados no pueden mediante inteligencia artificial recopilar, procesar o transferir los datos cubiertos de manera que se discrimine por motivos de raza, color, religión, origen nacional, sexo, orientación sexual o discapacidad. Esto no impide que los sujetos obligados segreguen un grupo de solicitantes, participantes o clientes. El proyecto de ley también obliga que los grandes titulares de datos que utilizan algoritmos evalúen sus algoritmos anualmente y presenten evaluaciones anuales de impacto algorítmico ante la FTC. Estas evaluaciones deben describir las medidas que la entidad ha tomado o tomará para mitigar los daños potenciales de los algoritmos, incluyendo cualquier daño específicamente relacionado con los menores de edad. Estas evaluaciones también tienen que tratar de

mitigar los daños algorítmicos relacionados con la publicidad para la vivienda, la educación, el empleo, la atención sanitaria, los seguros o el crédito, el acceso a los lugares de alojamiento público o las restricciones a los mismos, y cualquier impacto dispar en función de la raza, el color, la religión, el origen nacional, el género, la orientación sexual o la condición de discapacidad de una persona.

26. Como hemos adelantado, la Comisión Federal de Comercio (FTC) se encargará de hacer cumplir la norma. Además, la FTC asumirá algunas obligaciones nuevas, como el mantenimiento de un registro de intermediarios de datos o *data brokers* y la gestión de los mecanismos de exclusión voluntaria de la publicidad dirigida y de otros servicios de intercambio de datos. Y, una vez transcurridos cuatro años tras la entrada en vigor de la ley, las personas o grupos de personas podrán presentar una demanda civil ante un tribunal federal para reclamar daños y perjuicios, medidas cautelares, los honorarios razonables de los abogados y las costas del litigio.

V. Conclusiones

27. En este trabajo hemos puesto de manifiesto que las vigentes leyes federales relacionadas con la privacidad y protección de los datos son una serie de dispares leyes y reglamentos aplicados por varias agencias con diferentes jurisdicciones. Su obsolescencia y falta de adecuación a la sociedad digital, a lo cual se suma su funcionamiento práctico muy ineficiente, ha llevado a más de dos docenas de Estados a iniciar los trabajos legislativos en la materia, y cinco Estados ya han promulgado leyes estatales completas de privacidad y protección de datos de sus ciudadanos. Y más allá de los Estados, existe un consenso global en el país de aprobar una nueva legislación nacional de protección de datos. Ello ha desembocado en la presentación, con fecha 3 de junio de 2022, del proyecto de ley conocido como la *American Data Privacy and Protection Act* (ADPPA).

28. Este proyecto de Ley de Privacidad y Protección de Datos de Estados Unidos sienta las bases para poder promulgar por fin una legislación exhaustiva en la materia a escala federal en los Estados Unidos, al ser una iniciativa legislativa bipartidista y bicameral. Pretende minimizar la recopilación y el intercambio de datos en general, y de los menores de edad en particular. Impone obligaciones claras y viables a las empresas y otras organizaciones que recogen, utilizan y comparten datos personales. Incorpora un conjunto de salvaguardias básicas de privacidad y seguridad, incluidos los derechos individuales de acceso, supresión, portabilidad y rectificación de los datos personales, así como los derechos de exclusión de la publicidad dirigida y las transferencias de datos, sin olvidar unas cautelas básicas frente al uso de decisiones algorítmicas por medio del conjunto de herramientas agrupadas bajo el paraguas tecnológico de la inteligencia artificial (IA).

29. Sin embargo, el proyecto de ley ha desaprovechado la ocasión para crear una agencia independiente para consolidar la jurisdicción en esta materia reconocida las leyes de privacidad existentes y hacer cumplir la nueva legislación, destacadamente la propia ADPPA. La creación de esa agencia hubiera sido un paso muy relevante para garantizar la seguridad de los consumidores y la competencia en el mercado a medida que la economía digital y global siguen expandiéndose.