LA INSEGURIDAD EN LA PROTECCIÓN DE DATOS CONDUCE A LA INJUSTICIA ECONÓMICA

MICHELE GILMAN
Catedrática de Derecho, University of Baltimore

Con la Casa Blanca y el Congreso en manos de los demócratas, es muy probable que Estados Unidos pueda aprobar finalmente una ley federal de privacidad después de casi medio siglo de tentativas infructuosas (este es el cuarto intento en 45 años). En esta ocasión, incluso el *lobby* tecnológico está a favor de la medida, después de años de oposición.

El reciente apoyo bipartidista a la legislación sobre privacidad –encarnado por ejemplo por el presidente republicano del Comité de Comercio del Senado, Roger Wicker, y su contraparte demócrata Frank Pallone, busca dar respuesta a una creciente desconfianza por parte del público acerca de las nuevas tecnologías, que podría desembocar en un potencial *techlash* (la reacción contra el exceso digital), debido a un goteo constante de casos de sustracciones de datos y de campañas de desinformación en las redes sociales. La concordancia de los dos partidos en una nueva legislación también busca poner orden en el galimatías de leyes estatales que siguió la estela del estado de California, que aprobó una legislación propia sobre esta materia en 2018.

Parece pues que es este el momento oportuno para promulgar una nueva ley, ahora que, además, contamos con multitud de evidencias de que la privacidad de los datos es también un factor importante de justicia económica. En base a mi trayectoria como catedrática de Clínica Jurídica y abogada con más de dos décadas de experiencia representando a personas con ingresos bajos, he visto de primera mano cómo difiere la consciencia de la privacidad digital en función de la clase social a la que se pertenece. Y sin duda, son los estadounidenses pobres los que se exponen a más riesgos.

Segmentación de datos

Tomemos como punto de partida los corredores de datos o *data brokers*, nombre que reciben las compañías que venden datos personales recopilados de fuentes[1] como los registros públicos, la navegación por Internet, lo publicado en las redes sociales, los correos electrónicos, las apps utilizadas y las tarjetas de fidelización en el comercio minorista. Esta floreciente industria es una de las razones que explican porque los consumidores se ven bombardeados con anuncios *online* de productos a los que tal vez solo han echado un breve vistazo. Para la mayoría de las personas esto es simplemente una pequeña molestia cotidiana, pero para las personas de ingresos bajos, los perjuicios van más allá del hastío que todos compartimos por su insistente pesadez.

Los expedientes digitales reunidos por los corredores de datos, por ejemplo, se utilizan para identificar a los estadounidenses de ingresos bajos[2] y hacerles ofertas en condiciones abusivas de préstamos, hipotecas a alto interés y programas de formación, que van contra sus propios intereses y que rozan la estafa. Estos corredores segmentan a los consumidores en categorías muy concretas y bastante reveladoras, como "rural que apenas llega a fin de mes" o "ahogados por los créditos: familias urbanas"[3].

A pesar de que a resultas de una serie de demandas legales Facebook se vio obligada a impedir que sus anunciantes segmentasen por grupos a sus potenciales clientes en función de criterios como el género, la raza, el código postal o la edad, los anunciantes aún pueden seguir discriminando a determinadas personas, simplemente, porque son pobres. La pobreza no es una categoría protegida por las leyes sobre derechos civiles ni por la Constitución de EEUU.

Mientras, la policía utiliza las grandes bases de datos masivos existentes para predecir la actividad criminal, con un foco especial en los barrios de renta baja y habitados mayormente por minorías. Uno de los problemas de esta práctica es que crea un círculo vicioso por el que aquellas comunidades que están más fuertemente vigiladas por la policía son también las que más alimentan el *software* predictivo que insta a una vigilancia policial más agresiva[4].

Datos y exclusión social

La segmentación de los datos no es el único problema. El *big data* también puede emplearse para excluir a las personas que se encuentran en situación de pobreza material de oportunidades que podrían favorecer su estabilidad económica. Por ejemplo, algunos empresarios utilizan ya sistemas de rastreo de los solicitantes de empleo para recopilar información y predecir si un candidato potencial realizará bien su trabajo. Del mismo modo, también las universidades están testando algoritmos para determinar qué estudiantes potenciales tienen más probabilidades de quedarse hasta la graduación. También algunos propietarios inmobiliarios recurren ya a informes de evaluación de futuros posibles inquilinos para predecir si pagarán puntualmente el alquiler.

Y si bien estos pueden ser objetivos legítimos, la sociedad pone demasiada fe en los algoritmos utilizados para predecir la conducta humana. Puede que los dictámenes que salen de un ordenador tengan una pátina de objetividad, pero la realidad es que son personas de carne y hueso las que imprimen sus propios sesgos –conscientes o inconscientes– en el *software* y en las bases de datos que alimentan estas predicciones, lo que puede reforzar prejuicios cada vez más arraigados. Además, muchos de los datos utilizados en los algoritmos pueden perfectamente ser erróneos[5]. Dado que los algoritmos incluyen cada vez más información extraída de las redes sociales, la gente puede acabar siendo juzgada por lo que publican en ellas sus "amigos".

1. Véase, por ejemplo, Ingliss, J. "Your smartphone apps are tracking your every move: 4 essential reads". *The Conversation*, 11 de diciembre de 2018.
2. Véase, por ejemplo, el capítulo dedicado a este tema en el informe "Civil Rights, Big Data, and Our Algorithmic Future". The Leadership Conference on Civil and Human Rights, septiembre de 2014.
3. En relación con los procesos de segmentación, véase Taube, A. "How Marketers Use Big Data To Prey On The Poor". *BussinessInsider*, 19 de diciembre de 2013.
4. Véase, por ejemplo, Haskins, C. "Dozens of Cities Have Secretly Experimented With Predictive Policing Software". Vice, 6 de febrero de 2019.
5. Véase, a este respecto, Jagadish, H. V. "Big Data analyses depend on starting with clean data points". *The Conversation*, 4 de agosto de 2015.

Por otra parte, a consecuencia de la pandemia de la COVID-19, millones de familias están pasando dificultades económicas, y el rastro digital que dejan los desahucios, los impagos en las tarjetas de crédito o en las facturas de los servicios públicos quedará registrado en su perfil digital durante muchos años, haciendo que les resulte aún más difícil recuperar su equilibrio económico una vez que remita la emergencia de salud pública. Sin embargo, la falta de transparencia implica que estas personas nunca sabrán por qué se les niega un trabajo, una vivienda o una educación. Hasta la fecha, los mecanismos para corregir los datos perjudiciales o bien no existen o son tan kafkianos que la gente se siente frustrada y abandona la tramitación antes de obtener resultados.

A estas alturas, no debería sorprendernos que en aquellos estados de EEUU que emplean los algoritmos para evaluar la elegibilidad para recibir prestaciones públicas –como el *Medicad*, que da asistencia sanitaria a personas con bajos ingresos– miles de personas perfectamente cualificadas para obtener ayudas hayan sido expulsadas de los programas, poniendo en peligro su salud y, en algunos casos, su vida. Sabemos además que estos sistemas han acusado injustamente a miles de personas de cometer fraude[6]. El consiguiente estrés financiero sobre los acusados ha tenido como resultado desahucios, divorcios, valoraciones crediticias denegadas, gente que acaba viviendo en la calle y quiebras por insolvencia. Y es que la toma de decisiones automatizada despoja a la prestación de servicios sociales de la capacidad de contemplar matices que son tremendamente importantes.

La seguridad de los datos

La seguridad de sus datos es otra área de preocupación para los estadounidenses con ingresos bajos. Recientemente, un grupo de expertos en seguridad digital han localizado una base de datos en Internet que contenía información personal acerca de nada más y nada menos que 80 millones de hogares norteamericanos[7]. La existencia de esta base de datos responde a años de filtraciones de seguridad, exponiendo a dos de cada tres hogares estadounidenses al riesgo de un robo de identidad. Si bien es cierto que estas filtraciones son una pesadilla para todos, pueden ser devastadoras en especial para aquellas personas que viven con sus finanzas al límite. Generalmente no pueden permitirse las costosas y complicadas medidas necesarias para limpiar su crédito después de que alguien les haya robado la identidad. Las pérdidas económicas resultantes de una de estas filtraciones de información pueden empujar a una persona con bajos ingresos a la bancarrota financiera. Por otra parte, el robo de identidad puede exponer también a las personas con bajos ingresos a sufrir un arresto injusto, a que les recorten el suministro en un servicio público, o a ser objeto de tácticas agresivas de cobro de deudas.

Brechas en la privacidad de los datos

En el caso de EEUU, la mayoría de estos perjuicios se explican por el hecho de que el país todavía carece de una ley general de protección de la privacidad. Aunque los 50 estados exigen ya a las compañías que notifiquen a sus consumidores las filtraciones que se produzcan, solo unos cuantos estados, incluidos California y Virginia, han tomado medidas para regular cómo se recopilan y utilizan los datos personales. Ante la inacción del Congreso, otros estados están considerando adoptar una legislación similar.

Por el momento, existen unas cuantas leyes sectoriales federales[8] que protegen determinados tipos de información financiera y sanitaria de los ciudadanos norteamericanos. Sin embargo, el actual régimen de notificación y consentimiento carga sobre las personas la responsabilidad de salvaguardar su propia privacidad. Y las compañías cuentan con el hecho de que los consumidores no leen atentamente los inacabables pliegos de condiciones, cada vez que uno accede a un nuevo sitio web.

Lecciones de Europa

Los legisladores estadounidenses que trabajan en la redacción de una ley de privacidad federal deberían buscar inspiración en lo que hace Europa. El año 2018, la Unión Europea empezó a implementar el Reglamento General de Protección de Datos (RGPD), que confiere a sus ciudadanos una serie de derechos sobre el control de sus datos. En particular, también incluye disposiciones que podrían mejorar sensiblemente la privacidad de las personas con ingresos bajos. El Reglamento General prohíbe, por ejemplo, determinados tipos de creación automatizada de perfiles. Esto podría poner freno a los perfiles que limitan el acceso de la gente a empleos, vivienda y otros servicios necesarios por motivos ilegítimos. La ley también confiere a la gente el derecho a una explicación acerca de una decisión tomada de manera automatizada, lo que podría aportar algo de luz sobre los oscuros procesos de selección automatizada, permitiendo además el ejercicio de una reclamación justificada. La ley incluye también el *derecho al olvido*, que exige que los datos personales sean borrados cuando ya no son necesarios para el propósito original por el que se recopilaron, o cuando una persona solicita que sean borrados. Fundamentalmente, esto implica hacer borrón y cuenta nueva de registros cuando la situación financiera mejora. Por si fuera poco, la ley cuenta con un régimen de sanciones e imposiciones en caso de incumplimiento, y requiere de participación pública en las políticas de datos establecidas por las grandes empresas. En el largo plazo, y pese a sus muchas bondades, el RGPD solo será efectivo para los ciudadanos de la UE si se hace cumplir rigurosamente.

Este es el momento adecuado para que Estados Unidos adopte disposiciones similares, encaminadas a mejorar el control de los estadounidenses sobre sus datos personales. La prioridad debe ser asegurarnos de que las tecnologías datocéntricas actúan a favor de las personas y no contra ellas.

6. Véase Gilman, M. "AI algorithms intended to root out welfare fraud often end up punishing the poor instead". *The Conversation*, 14 de febrero de 2020.
7. Morris, Ch. "'A Goldmine for Identity Thieves': Unprotected Database Puts 65% of American Households At Risk". Fortune, 29 de abril de 2019.
8. Para más detalles acerca de las leyes sectoriales, véase Solove, D. "The Growing Problems with the Sectoral Approach to Privacy Law". TeachPrivacy, 13 de noviembre de 2015.