Luminate
Construyendo sociedades más fuertes

La Delusión de los Datos: la protección de los datos personales no es suficiente cuando el daño es colectivo

Autor: Martin Tisné, Director Ejecutivo, Luminate

Editor: Marietje Schaake, Directora de Políticas Internacionales,
Centro de Políticas Cibernéticas de la Universidad de Standford.

Julio de 2020

La amenaza de la discriminación digital

El 17 de marzo de 2018, estallaron las preguntas sobre la privacidad de datos a raíz del escándalo de la anteriormente desconocida consultora Cambridge Analytica. Los legisladores todavía están intentando actualizar las leyes para contrarrestar los daños del Big Data y la Inteligencia Artificial.

En marzo de 2020, la pandemia de COVID-19 puso en el centro del debate público las dudas sobre la suficiencia de las seguridades jurídicas y planteó advertencias urgentes sobre las implicancias respecto de la privacidad de las aplicaciones de rastreo de contactos[1]. Sin embargo, las consecuencias de la vigilancia de los efectos de la pandemia son aún mayores que cualquier aplicación: el transporte, la educación, los sistemas de salud y las oficinas se están convirtiendo en grandes redes de vigilancia. Si solo consideramos los balances individuales entre los sacrificios de privacidad y los supuestos beneficios de salud, olvidaremos lo central. La naturaleza colectiva del big data implica que la gente está más afectada por los datos de terceros que por los propios. Al igual que con el cambio climático, la amenaza es a nivel sociedad y personal.

En la era del big data y la inteligencia artificial, la gente puede sufrir por la manera en que la suma de datos individuales se analiza y clasifica en grupos por medio de algoritmos. Como consecuencia, están apareciendo nuevos tipos de daños colectivos basados en datos: publicidad en línea sobre viviendas, trabajos y créditos que discriminan sobre la base de la etnia y género, mujeres descalificadas de sus trabajos por su género y actores extranjeros intentando radicalizar grupos de derecha *light* y empujándolos hacia la extrema derecha.[2]

Nuestro debate público, nuestros gobiernos y nuestras leyes se encuentran mal preparados para lidiar con estos daños colectivos -en lugar de individuales.

Los datos son el nuevo CO_2

Al igual que con el CO_2, la privacidad de datos va mucho más allá de la persona. Somos prisioneros del consentimiento de los otros. Si uno compara los daños basados en datos con aquellos producidos por el CO_2, se observa claramente cómo los impactos son a nivel sociedad y no individual. Las emisiones del auto de mi vecino, el humo de una fábrica en otro continente, me afectan más de lo que mi pequeña huella de carbono jamás lo hará. Esta amenaza colectiva al cambio climático se refleja perfectamente en la ley ambiental y respalda la lógica (política) de las reducciones de emisiones y los acuerdos de París.[3]

Los individuos pueden disfrutar de beneficios a corto plazo de aquello que provocará daños de manera colectiva en el largo plazo. Para pensar de manera optimista, la Coronacrisis podría abrir el camino a leyes que traten sobre daños colectivos basados en los datos. Lo más probable es que el conflicto entre los miedos inmediatos y comprensibles de la sociedad respecto del sistema de salud se opondrá a las protecciones de la privacidad. Por ejemplo, el ministro de salud del Reino Unido dijo que "nadie debería restringir su trabajo en respuesta al coronavirus a causa de las leyes de protección de datos".[4] Incluso la Estrategia de Datos de la Comisión Europea se centra principalmente en darles poder a los individuos con respecto a "sus" datos.[5] La necesidad de derechos sobre datos colectivos continúa siendo ignorada.

"La naturaleza colectiva del big data implica que la gente está más afectada por los datos de terceros que por los propios. Al igual que con el cambio climático, la amenaza es a nivel sociedad y personal".

De los derechos colectivos a los individuales y viceversa

Los derechos sobre datos no estaban históricamente tan individualizados como lo están hoy en día. El derecho sobre los derechos humanos a finales de la Segunda Guerra Mundial se centraba mayormente en la protección de grupos. El régimen Nazi había oprimido y masacrado judíos, gitanos roma y otros pueblos perseguidos solo por pertenecer a un grupo minoritario. El daño colectivo causado por un estado pernicioso se articuló con el concepto de genocidio: un nuevo concepto para describir los crímenes cometidos "con intención de destruir, en su totalidad o en parte, un grupo nacional, étnico, racial o religioso". El objetivo era por tanto proteger a los grupos de crímenes genocidas futuros.[6]

En la década de 1970, el péndulo comenzó a balancearse en dirección a la privacidad individual, con el surgimiento de la computación. La Organización para la Cooperación y el Desarrollo Económicos (OCDE) desarrolló un conjunto de pautas sobre privacidad en 1980. Estas pautas popularizaron la noción de que los individuos deberían brindar su consentimiento informado para todo tipo de información utilizada sobre ellos y para ellos.[7] Durante el mismo período, la ley de protección de datos francesa de 1978 consagró la noción de que los datos personales de las personas deben ser recogidos y procesados de manera justa y lícita con fines específicos, explícitos y legítimos, y con el consentimiento de la propia persona (a la que se refiere como "persona interesada").[8] La ley francesa a su vez inspiró la Directiva de la Unión Europa de 1995 sobre la protección de los datos personales, que inspiró el Reglamento General de Protección de Datos de 2018 (RGPD) frecuentemente llamado la regla de oro de las leyes sobre protección de datos. Hoy en día, los derechos de datos son vistos como "derechos individuales" y la individualización de los derechos de datos se ha convertido en un pilar de las leyes sobre protección de datos alrededor del mundo.[9]

La ironía de la historia es que a medida que los gobiernos y las leyes se desplazaban de la protección de grupos a la protección de individuos, las empresas de tecnología se movían en la dirección contraria, del análisis del comportamiento individual hacia el de los grupos. La era del aprendizaje automático efectivamente hace que la negación individual del consentimiento sea insignificante. Aun si me rehúso a utilizar Facebook o Twitter o Amazon, el hecho de que todos a mi alrededor los usen implica que haya igual cantidad de puntos de datos sobre mí disponibles.

> **"La era del aprendizaje automático efectivamente hace que la negación individual del consentimiento sea insignificante."**

A medida que los ingenieros y las empresas comenzaron a implementar algoritmos cada vez más complejos, sumado a los datos recopilados a escala, el mercado pasaba de gestionar datos individuales a extraer valor de datos colectivos. El hecho de que las leyes sigan centradas en el individuo hace que estén desfasadas con la realidad que crean la tecnología y la inteligencia artificial y que evoluciona rápidamente. Nuestras sociedades precisan derechos de datos a nivel colectivo e individual, de manera similar a las leyes contra la discriminación que protegen a individuos y a grupos.[10]

Por qué la falacia individualista le conviene al Big Tech

Cuando el profesor de diseño de medios David Carroll buscaba obtener datos sobre sí mismo de Cambridge Analytica, presentó una demanda en virtud de la ley de protección de datos del Reino Unido. El Prof. Carroll luego objetó la liquidación de la empresa fundamentando su objeción en el interés público por la responsabilidad y la supervisión

“Aun si me rehúso a utilizar Facebook o Twitter o Amazon -el hecho de que todos a mi alrededor los usen implica que haya igual cantidad de puntos de datos sobre mí disponibles.”

independiente. Los documentos judiciales muestran que él creía que el enterarse más sobre cómo sus datos personales eran recopilados y usados aclararía el impacto del big data y la inteligencia artificial en el conjunto bajo un régimen democrático. Su apelación fue desestimada.[11] El caso muestra lo difícil que es para los individuos iniciar acciones legales por daños colectivos, a diferencia de acciones por invasiones de la privacidad personal.

El valor de los datos de un individuo para Google o Facebook es marginal. Para las empresas, el valor radica en las inferencias que se puedan hacer a partir de su interacción con otros.[12] En 2018, Facebook generó ingresos de USD10/año por usuario diario activo.[13] Los daños que el individuo puede demostrar son por tanto mínimos. La combinación de individuos en una clase y el seguimiento de las respuestas de esa clase a los diferentes estímulos significa que Google no puede decir cuántos datos sobre una persona han sido usados. Pero el valor de su procesamiento de datos colectivos es enorme. De esos USD10 por persona por año, Facebook generó un ingreso neto anual de USD22.000 millones en 2018 mientras que Alphabet generó USD30.000 millones. PwC reveló que las compañías con prestaciones analíticas tenían valores de cotización en bolsa mayores que sus pares dentro de la misma industria.[14]

Las leyes y el pensamiento desarrollados en la década de 1970 ya no son adecuados para lidiar con la realidad de hoy día. El punto acá es la disparidad fundamental entre la lógica del mercado y la lógica de la ley.[15] Los mercados de tecnología contemporáneos extraen valor de los datos colectivos. Nuestras leyes responden a daños individuales y no han cambiado para reflejar los cambios en la tecnología. Los gobiernos deberían cambiar los regímenes legales para acompañar la lógica del mercado. Capaz no ha habido tanta urgencia hasta ahora debido a que la naturaleza de los daños colectivos -similar a la contaminación producida por CO_2- es invisible a la persona promedio. Los algoritmos se mantienen en secreto, sus efectos omnipresentes pero invisibles. La noción de injusticia, que puede llevar a una mayor concientización y demandas legales, es evanescente cuando la injusticia se produjo de manera invisible por un modelo informático (aunque diseñado por seres humanos).[16] Por ello, es también menos probable que se produzca una acción colectiva.[17] La tarea en cuestión es comprender la naturaleza de los nuevos daños y tornar visible lo invisible.

Hacer visible lo invisible: daños basados en datos colectivos

Cuanto más colectivo el daño, menos gente está protegida y menos visible es el daño. Cuanto más individual el daño, más visibles son sus impactos y más gente se encuentra legalmente protegida. Si una persona es discriminada por pertenecer a un grupo protegido ya sea por su edad, género o etnicidad, será visible para ellos y estará, con suerte, en una posición de solicitar un resarcimiento. Cuando una persona es discriminada por una decisión algorítmica, es probable que sea menos visible y, actualmente, difícil reclamar un resarcimiento.[18]

La gente tiende a sufrir daños basados en datos de tres maneras principales. En primer lugar, son daños puramente individuales. Por ejemplo, a un individuo lo consideran no apto para un empleo a causa de datos directamente referidos a él/ella (por ejemplo, su edad). Las protecciones contra este tipo de daños están bien establecidas en la ley.

En segundo lugar, hay daños inferidos. Esto se da cuando se infiere que el individuo es parte de un grupo o categoría de personas, pero la persona cuyos datos son utilizados no se

ve perjudicada. Pensemos en personas que suben fotos públicas de ellos mismos en un sitio web de citas de los EE.UU., y estas fotos son usadas por investigadores que desarrollan de manera controvertida algoritmos para establecer la sexualidad de las personas basándose en sus características faciales.[19] Los individuos cuyas fotos son utilizadas no son necesariamente los únicos perjudicados. Las personas cuya sexualidad es "identificada" (aunque sea falsamente) a través de estas técnicas son las perjudicadas por medio de inferencias realizadas como resultado de datos recolectados y procesados.[20]

En tercer lugar, existen daños optimizados. Estos son daños sufridos como resultado de la manera en que los sistemas de aprendizaje automático son optimizados. El algoritmo de YouTube llegó a la conclusión de que a las personas les atrae el contenido que es más extremo de lo que están viendo en ese momento y los lleva por un camino que, como ha escrito la académica y activista Zeynep Tufekci, podría ser inofensivo (desde salidas a trotar hasta ultra maratones) o dañino (desde reuniones políticas a teorías conspirativas).[21] Las personas son descriptas involuntariamente por el algoritmo. Al igual que con los sistemas de optimización, el algoritmo de YouTube se encuentra centrado decididamente en sus usuarios y no focaliza sus externalidades en no usuarios, grupos minoritarios y cualquier otra persona que no esté en el sistema (por ejemplo, la sociedad en general).

Los sistemas legales y los arsenales de políticas de nuestros países se encuentran mal preparados para responder a los últimos dos tipos de daños basados en datos. La protección de datos, en su estado actual, se basa en una relación entre los responsables y los interesados. A medida que la tecnología se vuelve más sofisticada, esa conexión entre responsables e interesados flaquea. No es siempre claro quién es el responsable ni cuál interesado ha sido dañado. Aparecerá un vacío jurídico -que probablemente ya exista- y la responsabilidad decrece.[22]

A medida que el mundo se traslada a la virtualidad a causa del coronavirus, las compañías y los gobiernos recopilarán mucha más información sobre las personas a través de la recolección de datos. Esto probablemente aumente el uso de decisiones automatizadas, por ejemplo, sobre cómo asignar recursos. Y con mayor automatización, habrá aún mayores implicancias sobre la equidad. El procesamiento de datos puede decidir quién puede tener acceso a la educación, al bienestar o al sistema judicial. Las investigaciones durante los últimos cinco años han demostrado cómo los impactos negativos de la toma de decisiones automatizada respecto de las personas recaen desproporcionadamente sobre aquellos que ya se encuentran marginados en la sociedad, como las personas de color, las mujeres y los inmigrantes.[23]

"Nuestras sociedades precisan derechos de datos a nivel colectivo e individual, de manera similar a las leyes contra la discriminación que protegen a individuos y a grupos."

La dificultad del siglo 21 respecto del problema de la privacidad de datos y la discriminación es que los miembros del público ya no saben a qué grupo pertenecen, sólo el algoritmo lo sabe. Muchas personas ni siquiera sabrán que están siendo discriminadas y que se está trazando un perfil sobre ellas.[24] La conversación necesita replantearse en torno a la automatización y el poder y sobre cuáles grupos se verán impactados negativamente.

Las soluciones radican en el mecanismo de *hard accountability*, esto es, en una estricta supervisión reglamentaria de la toma de decisiones basada en datos y en la habilidad de auditar e inspeccionar las decisiones y los impactos de los algoritmos en la sociedad.

Regular la automatización es regular el poder: el caso del mecanismo de *hard accountability*

Más que regular cómo la gente accede a que sus datos sean usados a fin de proteger su privacidad, los legisladores deberían regular la automatización comenzando con los algoritmos de caja negra que recopilan, ordenan y clasifican los datos. Eso implicará un método completamente nuevo de regulación. Los miembros del público necesitan información, escrutinio público y responsabilidad respecto de los impactos dispares de los grandes montos de automatización que reciben cada segundo del día.

"Las soluciones radican en el mecanismo de hard accountability, en una estricta supervisión reglamentaria de la toma de decisiones basada en datos y en la habilidad de auditar e inspeccionar las decisiones y los impactos de los algoritmos en la sociedad."

En la Unión Europea, el RGPD es débil respecto de la automatización y los daños colectivos.[25] La responsabilidad de los sistemas de decisiones algorítmicas se encuentra cubierta principalmente en los artículos 13-15 y 22 pero éstos están limitados a decisiones que son completamente automatizadas, que usan datos personales y que son consideradas "decisiones significativas" y por ello eluden muchos de los daños menores detallados anteriormente, que en conjunto equivalen a daños colectivos significativos.[26] Asimismo, el RGPD individualiza los daños basados en datos ya que le solicita a la persona que sufrió el daño que esté en el centro de cualquier reclamo que surja de ello. Eso sería como solicitar que un caso sobre las emisiones de CO2 de un país entero dependa de sus impactos comprobables en una persona.[27]

Se necesitan tres elementos para garantizar el mecanismo de *hard accountability*: (1) transparencia clara sobre dónde y cómo se toman las decisiones automatizadas[28] y su impacto en las personas y los grupos, (2) derecho de brindar aportes significativos del público y convocar a las autoridades para justificar sus decisiones, y (3) capacidad para aplicar sanciones.[29] El Proyecto de Ley de Datos de Interés Público debería encapsular estos tres puntos.

Transparencia clara

El foco debería estar en el escrutinio público de la toma de decisiones automatizadas y en los tipos de transparencia que conducen a la rendición de cuentas.[30] Esto incluye la revelación de datos de capacitación y de objetivo ya existentes detrás de los algoritmos, al igual que sus impactos, independientemente de que conduzcan a resultados dispares, y afecten a distintos grupos. La transparencia clara y dirigida explica los algoritmos y las instituciones que los usan. Por ejemplo, revelan información sobre desempeño institucional (por ejemplo: uso de cámaras de reconocimiento facial por la policía y su impacto) y son explícitos sobre lo que es medido, por quién y cómo. Pero la transparencia continúa siendo una condición necesaria pero no suficiente para la responsabilidad.[31] Para ello se necesitan un aporte significativo del público y la posibilidad de imponer sanciones.

Participación pública

El público tiene un derecho fundamental de convocar a aquellos en el poder para que justifiquen sus decisiones. Este "derecho a exigir respuestas" no debería verse limitado a la participación consultiva en la que a las personas se les pide su aporte y los funcionarios pasan a otro tema. Debería incluir la participación empoderada en la que el aporte del público es exigido con anterioridad al lanzamiento de un algoritmo en la sociedad. Por ejemplo, las evaluaciones de impactos algorítmicos deberían brindar a los miembros

> “De manera similar a la naturaleza colectiva de la amenaza de cambio climático, nuestros gobiernos y legisladores deben cambiar la manera de pensar sobre la respuesta reguladora.”

del público la posibilidad de dar un aporte significativo sobre el uso de la toma de decisiones automatizadas, y expandir dichas evaluaciones como una herramienta para la toma de decisiones basadas en la comunidad.

Sanciones

Finalmente, el poder de imponer sanciones es clave para que estas reformas sean exitosas y para lograr la rendición de cuentas. El RGPD se ha visto restringido por la falta de financiamiento y capacidad de los comisarios encargados de la protección de datos en Europa. A pesar del poder del RGPD de imponer multas de hasta 4% del volumen de ventas de una compañía, pocas de esas multas han sido asignadas y la mitad de los reguladores europeos de protección de datos solo tiene cinco o menos expertos técnicos.[32] Pero las comisiones de información o protección de datos no pueden ser únicamente responsables por la rendición de cuentas de los algoritmos a medida que nuestras sociedades son transformadas por la inteligencia artificial. Las compañías y los gobiernos necesitan leyes que restrinjan la automatización y el uso de datos, más allá de las implicancias respecto de los datos personales de las personas. Para ello, las sociedades necesitarán también de la modernización de las leyes sectoriales tales como la ley de trabajo, la ley penal, la ley de genética, la ley ambiental y la ley de discriminación.[33] Por ejemplo, las leyes que regulan la administración pública ya podrían aplicarse aquí. Podría usarse la ley administrativa para ordenar una mayor responsabilidad de la toma de decisiones automatizadas usada por el sector público.[34] Las leyes laborales podrían adaptarse para responder por el rol de la tecnología en la gestión de las relaciones empleador/empleado.[35]

Precedentes

Existen ejemplos de proyectos de ley que han buscado llenar este vacío. En los Estados Unidos de América, se realizó un esfuerzo en 2019 para sancionar la Ley de Responsabilidad Algorítmica que finalmente quedó paralizada en el Congreso y que apuntaba a determinar si los algoritmos del sector privado llevaban o no a la discriminación. La Ley hubiera exigido a las empresas realizar evaluaciones de impacto algorítmico en determinadas situaciones para comprobar la presencia de prejuicios o discriminación.[36] En Francia, la Ley Digital de la República (*Loi Pour Une République Numérique*) se aplica hoy en día a las decisiones administrativas tomadas por los sistemas algorítmicos del sector público, pero podría brindar un proyecto para leyes futuras. Brinda acceso a la importancia de la automatización respecto de la decisión final. También facilita el acceso a datos usados y su fuente, así como a cualquier ponderación y parámetro de tratamiento en caso de ser utilizado en decisiones que afectaron a las personas y brinda información sobre el resultado del proceso automatizado. Por el contrario, el RGPD establece restricciones, pero sólo respecto del uso de datos personales en decisiones totalmente automatizadas.[37]

Conclusión

Las preocupaciones sobre la privacidad en torno al COVID-19 revelaron una cantidad de incompatibilidades sistémicas entre el derecho de la privacidad individual y el valor del procesamiento de datos colectivos. La pandemia acelera el riesgo de desigualdad y se aceleran dramáticamente nuevos daños como la vigilancia y la recolección de datos en pos de poner fin a la crisis sanitaria. La mayoría de los que sufren ya estarán marginados y serán vulnerables en nuestras sociedades. De manera similar a la naturaleza colectiva de la amenaza de cambio climático, nuestros gobiernos y legisladores deben cambiar la manera de pensar sobre la respuesta reguladora. Necesitan considerar el impacto tanto colectivo como individual de los datos.

Proyecto de ley de datos de interés público

Transparencia clara

Requerir que las empresas y los gobiernos faciliten los datos y códigos fuente detrás de los algoritmos de alto riesgo y definan cuáles son considerados "de alto riesgo" en relación con las pruebas sobre los impactos dispares de dichos algoritmos en la población (por ejemplo, si recaen desproporcionadamente sobre comunidades marginadas).

Requerir que las empresas y los gobiernos publiquen las valoraciones de los impactos algorítmicos que evalúan los resultados del tratamiento algorítmico sobre grupos, así como los daños colectivos basados en datos. Garantizar que los resultados de dichas evaluaciones sean publicados en forma transparente. Garantizar que preceden la implementación de la utilización de la inteligencia artificial de alto riesgo y renovarlo de manera regular.[38]

Garantizar la transparencia plena y la responsabilidad de la automatización:

- Las modificaciones de los algoritmos que podrían parecer pequeñas o insignificantes en solitario pueden tener como resultado un impacto colectivo sustancial al ser tomados juntos -estos estarían incluidos. Esto no debería limitarse a "decisiones" realizadas por un algoritmo ni a aquellas decisiones que necesitan ser "significativas" como es el caso actual con el artículo 22 del RGPD[39].
- Aplicar ambos a decisiones tanto total como parcialmente automatizadas.[40]
- Requerir transparencia y rendición de cuentas por la forma en que una decisión fue tomada basada en un modelo informático, sin explicar simplemente el modelo en abstracto. (El nivel y el modo de contribución del procesamiento algorítmico respecto de la decisión tomada.[41])
- Abarcar las decisiones más allá de aquellas que usan datos personales. Por ejemplo, esto cubriría autos autónomos o datos que fueron alguna vez personales y luego supuestamente anonimizados. Las personas se ven afectadas por datos que no son personales y por datos personales que no son sobre ellos.

Participación pública

Brindar a los miembros del público la posibilidad de dar un aporte significativo al uso de la toma automatizada de decisiones (lo que incluye, a modo ilustrativo, aportes a las evaluaciones de impacto algorítmico).

Garantizar que la participación del público sea empoderada y no meramente consultiva.

Sanciones

Garantizar la capacidad para imponer sanciones por falta de cumplimiento.

Financiar y obtener recursos para entidades responsables de la rendición de cuentas, lo que incluye órganos de supervisión para leyes sectoriales tales como la ley laboral, la ley penal, la ley de genética, la ley ambiental y la ley contra la discriminación, además de agencias de protección de datos.

Importancia tanto para los grupos como para los individuos

Permitir que tanto las personas como las organizaciones puedan formular peticiones.[42]

Brindar acceso a parámetros de tratamiento y, en caso de ser apropiado, sus ponderaciones, aplicadas a la situación de la(s) persona(s) o grupos correspondientes.

Sobre el autor

Martin Tisné es el Director Ejecutivo de Luminate, una organización filantrópica global. Es responsable del área de impacto de Derechos Digitales y de Datos, del trabajo en Europa y de las políticas y la defensa de Luminate. Junto a la administración de Obama, Martin fundó la Alianza para el Gobierno Abierto [*Open Government Partnership*] y ayudó a hacerla crecer hasta transformarse en una iniciativa de más de 70 países. También inició la Carta Internacional de Datos Abiertos, la Carta del G8 de Datos Abiertos y el compromiso del G20 con los principios de datos abiertos. Martin es cofundador de Publish What You Fund, una campaña global para la transparencia en la ayuda internacional y de Integrity Watch Afghanistan, la ONG de anticorrupción líder del país. Twitter: @martintisne

Sobre la editora

Marietje Schaake es la directora de políticas internacionales en el Centro de Políticas Cibernéticas [*Cyber Policy Center*] de la Universidad de Stanford y es miembro investigadora de políticas internacionales en el Instituto para la Inteligencia Artificial Centrada en el Ser Humano [*Institute for Human-Centered Artificial Intelligence*] de la Universidad de Stanford. Fue nombrada presidente del Instituto para la Paz Cibernética [*Cyber Peace Institute*].

Entre 2009 y 2019, Marietje se desempeñó como Miembro del Parlamento Europeo para el partido liberal holandés donde se centró en políticas de tecnología, comercio, relaciones exteriores. Marietje se encuentra afiliada a un número de organizaciones sin fines de lucro, lo que incluye, el Concejo Europeo de Relaciones Exteriores y la Fundación de Investigación Observador [*Observer Research Foundation*] de la India. También escribe una columna mensual para el Financial Times y una columna bimensual para el diario holandés NRC.

Reconocimientos del autor

Estoy sumamente agradecido a Salmana Ahmed, Madeleine Clare Elish, Kate Crawford, Polly Curtis, Jonathan Fox, Janet Haven, Swee Leng Harris, Gus Hosein, Karen Levy, Jim Peacock, Ravi Naik, David Robinson, Marietje Schaake, Ben Scott y Sandra Wachter por revisar el borrador de este trabajo y por la gran ayuda de sus comentarios.

También me gustaría agradecer de manera especial a Adrien Abecassis, Julia Angwin,Azeem Azhar, Solon Barocas, Ailidh Callander, Simon Chignard, Sylvie Delacroix, Alix Dunn, Alex Goodman, Seda Gürses, Kieron O'Hara, Gry Hasselbalch, Carly Kind, Neil Lawrence, Sean Macdonald, Aiha Nguyen, Tanya O'Carrol, Reema Patel, Seeta Peña Gangadharan, Imogen Parker, Phil Sheldrake, Martha Spurrier, Katarzyna Szymielewicz, Linnet Taylor, Jeni Tennison, Zeynep Tufekci, Michael Veale, Henri Verdier, Stefaan Verhulst, Adrian Weller, Glen Weyl, Meredith Whittaker, y Caroline Wilson Palow por su asesoramiento. Estoy sumamente agradecido por el tiempo que me han dedicado.

Luminate

Luminate es una organización filantrópica mundial focalizada en el fortalecimiento de las personas y las instituciones para poder trabajar juntos a fin de construir sociedades justas. Apoyamos a las organizaciones y a los emprendedores innovadores y valientes alrededor del mundo, y abogamos por políticas y medidas que produzcan cambios en nuestras cuatro áreas de impacto: Empoderamiento Cívico, Derechos de Datos y Digitales, Transparencia Financiera y Medios Independientes. Trabajamos con nuestros socios para asegurar que todos tengan la oportunidad de determinar y participar en los temas que afectan a sus sociedades y para hacer que aquellos que ocupan cargos de poder sean más receptivos y responsables. Luminate fue creada en 2018 por los filántropos Pierre y Pam Omidyar. La organización fue fundada por The Omidyar Group.
www.luminategroup.com

Stanford | Cyber Policy Center
Freeman Spogli Institute

El Centro de Políticas Cibernéticas [*Cyber Policy Center*] en el Instituto Freeman Spogli de Estudios Internacionales [*Freeman Spogli Institute for International Studies*] es el centro principal de la Universidad de Stanford para el estudio interdisciplinario de temas vinculados a la tecnología, el gobierno y las políticas públicas. A través de investigaciones, compromiso político y enseñanza, el Centro de Políticas Cibernéticas trabaja para brindar soluciones innovadoras a los gobiernos nacionales, a las instituciones internacionales y a la industria.

Bibliografía

1 Ver John Thornhill, Naomi Klein.

2 Ali, Sapiezynski, Bogen, Korolova, Mislove y Rieke, "Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes", 2019 https://arxiv.org/abs/1904.02095

3 Más recientemente en Holanda, el caso Urgenda ("caso del clima") contra el Gobierno holandés estableció que el gobierno tenía una obligación legal de prevenir el cambio climático peligroso y debía reducir de manera significativa las emisiones a fin de proteger los derechos humanos.

4 https://twitter.com/MattHancock/status/1240189379676712960?s=20

5 https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy

6 Samantha Power, "A Problem From Hell", 2002

7 https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

8 https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf

9 Éstas varían desde el derecho a ser informado, el derecho a acceder a los datos, rectificarlos, eliminarlos, restringir su procesamiento. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT Según la Carta de Derechos Fundamentales de la Unión Europea: "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan".

10 Agradezco a la Prof. Sandra Wachter por este comentario. Por favor, ver "Affinity Profiling and Discrimination by Association in Online Behavioural Advertising" https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3388639

11 El juez de la liquidación asentó que "los "intereses" pertinentes eran los intereses del Prof. Carroll como acreedor, no sus intereses como académico curioso o como alguien que lidera una campaña para establecer un principio sobre el uso de los datos o como alguien que se encuentra inquieto por lo que pudiera haberle pasado a sus datos en el pasado. https://www.judiciary.uk/judgments/vincent-john-green-mark-newman-v-cambridge-analytica-uk-limited-others/

12 A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829

13 https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx

14 https://www.bennettinstitute.cam.ac.uk/publications/value-data-summary-report/; pwc.co.uk/issues/data-analytics/insights/putting-value-on-data.html

15 Ver Julie Cohen, "Between Truth and Power", 2019

16 Un estudio reciente sobre el uso de la Inteligencia Artificial al contratar en el Reino Unido determinó que las herramientas de auditoria utilizadas para garantizar el cumplimiento no podían determinar de manera exacta sesgos en el sistema de la Inteligencia Artificial. Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547922

17 Agradezco a Prof. Wachter por esta perspectiva.

18 Los pioneros en esta área incluyen a: E. Bloustein's "Group Privacy: The Right to Huddle" https://heinonline.org/HOL/LandingPage?handle=hein.journals/rutlj8&div=24&id=&page= ; Taylor, Floridi y van der Sloot (editores) de "Group Privacy: New Challenges of Data Technologies" https://www.springer.com/gp/book/9783319466064; Mittelstadt "From Individual to Group Privacy in Big Data Analytics" https://link.springer.com/article/10.1007/s13347-017-0253-7

19 https://www.law.ox.ac.uk/business-law-blog/blog/2018/10/right-reasonable-inferences-re-thinking-data-protection-law-age-big

20 Ver Dr. Sandra Wachter "A right to reasonable inferences: re-thinking data protection law in the age of big data and AI" https://www.law.ox.ac.uk/business-law-blog/blog/2018/10/right-reasonable-inferences-re-thinking-data-protection-law-age-big

21 https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html

22 Ver Ravi Naik, 2020 https://jolt.law.harvard.edu/digest/the-gentle-civilizer-of-technology

23 https://www.theguardian.com/technology/series/automating-poverty

24 "Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI" https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547922

25 https://gdpr-info.eu/

26 "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" Wachter, Floridi, Mittelstadt 2017 https://academic.oup.com/idpl/article/7/2/76/3860948; "Enslaving the algorithm: from a right to an explanation to a right to better decisions" Edwards y Veale 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3052831

27 La ley no permite que las ONGs reciban reclamos si esto no es ordenado por una persona específica (el "interesado") pero, nuevamente luego de mucha presión, esa parte de la ley se volvió opcional y solo tres de cada veintiocho países europeos eligieron sancionarla. Cuando las ONGs pueden presentar reclamos sistémicos en representación del público sin necesidad de tener un mandato de un individuo, los daños basados en daños podrían ser protegidos de manera colectiva de la misma manera que los daños ambientales lo son. Artículo 80 del RGPD. (2) El principal recurso del RGPD para contrarrestar los daños colectivos basados en datos es cuando la violación de los derechos individuales de la persona es sintomática de la misma violación sufrida por todos o cuando puede presentarse una demanda colectiva. Hay pocos de esos casos. Esa parte aparentemente incierta de la ley indica una tendencia futura potencialmente interesante. Estoy agradecido al equipo de Privacy International por el tiempo dedicado para explicar este punto.

28 A veces llamada "Ley Blade Runner" que requiere de un sistema automatizado o robot para declararse así misma como tal y no camuflarse como ser humano.

29 Ver la distinción entre los mecanismos de soft y hard accountability de Prof. Jonathan Fox's aquí: https://www.tandfonline.com/doi/full/10.1080/09614520701469955

30 https://luminategroup.com/posts/report/public-scrutiny-of-automated-decisions-early-lessons-and-emerging-methods

31 Jonathan Fox, "The uncertain relationship between transparency and accountability", 2007, https://www.tandfonline.com/doi/full/10.1080/09614520701469955; Fung, Graham, Weil "Full Disclosure: The Perils and Promise of Transparency", 2007

32 "GDPR accused of being toothless because of lack of resources", Financial Times 20 de abril de 2020, https://www.ft.com/content/a915ae62-034e-4b13-b787-4b0ac2aaff7e

33 Para una actualización del RGPD respecto de dichos temas, ver la conclusion de "A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI" https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829

34 Jennifer Cobbe, "Administrative Law and The Machines of Government", 2018 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3226913

35 En respuesta a la optimización usada en los trabajadores de Amazon, la mejor respuesta puede ser los derechos y protecciones de los trabajadores más que las leyes específicamente orientadas a la tecnología usada.

36 https://www.congress.gov/bill/116th-congress/house-bill/2231/all-info El proyecto de ley era un comienzo prometedor pero también criticado por depender del poder de ejecución relativamente débil de la Comisión Federal de Comercio [Federal Trade Commission], por no brindar una oportunidad a los aportes significativos del público como sí lo hacen las evaluaciones de impacto ambiental, y por no ordenar un nivel claro de transparencia pública para los resultados de las evaluaciones de impacto algorítmico.

37 La Ley Digital de la República (Loi Pour Une République Numérique) no está lo suficientemente investigada debido a que el campo de aprendizaje automático se encuentra excesivamente centrado en casos de estudios y ejemplos anglosajones. La ley hoy en día se aplica a decisiones administrativas tomadas por los sistemas algorítmicos del sector público, pero ofrece un proyecto para leyes futuras. La ley francesa brinda acceso a la importancia de la automatización para las decisiones finales. También facilita el acceso a datos usados y a su fuente, así como a cualquier ponderación y parámetro de tratamiento en caso de ser utilizado en decisiones que afectaron a las personas. También brinda información sobre el resultado del proceso automatizado. Por ejemplo, una persona podría tener acceso a datos y al código de fuente usado en un algoritmo que decidió asignarles o no un lugar en una universidad pública y cómo esa decisión fue tomada y ponderada (por ejemplo, ¿Fueron más importantes sus calificaciones que el lugar donde vivían?). Por el contrario, el RGPD establece restricciones, pero sólo respecto del uso de datos personales en decisiones totalmente automatizadas. También ver referencia a Edwards y Veale, 2018.

38 https://ainowinstitute.org/aiareport2018.html

39 Como dice Dr. Michael Veale "las decisiones que parecen "insignificantes" a nivel individual pueden realmente tener un gran impacto a nivel de grupo".

40 Las disposiciones del RGPD para la explicabilidad y responsabilidad de los algoritmos se encuentra restringida a decisiones que son 100% automatizadas. En la realidad, la mayoría de las decisiones automatizadas tienen a un ser humano involucrado en algún punto incluso cuando su involucramiento sea superficial o sustancialmente sesgado por el veredicto del algoritmo.

41 https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000031366350&idArticle=LEGIARTI000034195881

42 Ver nota 27