Digital Future Society

Hacia una mejor gobernanza de datos para todos:

Ética y privacidad de los datos en la era digital

Un programa de

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

MOBILE WORLD CAPITAL BARCELONA

Sobre Digital Future Society

Digital Future Society es una iniciativa transnacional sin ánimo de lucro que conecta a responsables políticos, organizaciones cívicas, expertos académicos y empresarios para explorar, experimentar y explicar cómo las tecnologías se pueden diseñar, usar y gobernar, a fin de crear las condiciones adecuadas para una sociedad más inclusiva y equitativa.

Nuestro objetivo es ayudar a los responsables políticos a identificar, comprender y priorizar los desafíos y las oportunidades fundamentales, ahora y en los próximos diez años, en relación con temas clave que incluyen la innovación pública, la confianza digital y el crecimiento equitativo.

Para más información visite digitalfuturesociety.com

Un programa de

Publicado
Abril 2020

Aviso legal
La información y las opiniones expuestas en este informe pertenecen al autor(es) y no reflejan necesariamente la opinión oficial de Mobile World Capital Foundation. La Fundación no garantiza la exactitud de los datos incluidos en este informe. Ni la Fundación ni ninguna persona que actúe en nombre de la Fundación será considerada responsable del uso que pueda darse a la información que contiene.

Nota a la versión en español
Este informe ha sido escrito en inglés y traducido al español. Digital Future Society apoya el uso de conceptos técnicos en español y se esfuerza por encontrar una traducción precisa, siempre que sea posible, sin comprometer por ello el significado original del contenido.

Contenido

Resumen Ejecutivo

El rápido desarrollo tecnológico actual plantea dilemas humanos y éticos. Las sociedades de todo el mundo están experimentando lo que se ha venido a llamar la cuarta revolución industrial, marcada por la eliminación de límites entre el mundo físico y el digital y la externalización de actividades y decisiones humanas, que se dejan a las máquinas, todo ello alimentado, en última instancia, por los datos.

Aunque no hay duda de que son una ventaja, los datos también pueden presentar riesgos éticos. La amenaza de la pérdida de privacidad y la creciente concienciación colectiva sobre el uso indebido de los datos han provocado fuertes debates sobre la necesidad de una mayor transparencia, responsabilidad e inclusión. Con intereses impulsados por las ganancias que aprovechan tecnologías cada vez más sofisticadas, los usuarios de datos, y en un sentido más amplio los ciudadanos, han dado la voz de alarma frente a los resultados nefastos que conlleva el uso poco ético de datos.

En un mundo cada vez más dependiente de algoritmos basados en datos que eligen y toman decisiones en nombre de los humanos, los responsables de formulación de políticas tienen la responsabilidad de garantizar que existan marcos regulatorios y mecanismos de gobernanza de datos adecuados para que los profesionales y usuarios de datos entiendan, respeten y puedan ejercer los derechos humanos fundamentales. Los responsables de formulación de políticas también tienen un papel fundamental a la hora de garantizar que todos los miembros de la sociedad posean las competencias necesarias para beneficiarse de los cada vez más frecuentes sistemas basados en datos.

El programa Digital Future Society colabora con expertos y responsables de formulación de políticas para expandir los límites del debate sobre ética digital y privacidad de datos y ha creado un espacio donde reflexionar y actuar sobre ciertas cuestiones, por ejemplo:

- ¿Cómo pueden las organizaciones prevenir los resultados poco éticos de las tecnologías basadas en datos?
- ¿Cómo pueden las administraciones públicas supervisar de manera ética responsable las tecnologías basadas en datos?
- ¿Cómo pueden los gobiernos apoyar el desarrollo de sistemas basados en datos que involucran la ciudadanía, ya que estos afectarán directamente a sus vidas?

La esencia de nuestra investigación no es otra que el deseo de crear una sociedad digital inclusiva en la que la ética y la privacidad de los datos sean la norma en lugar de excepciones o aspectos secundarios. Tras haber explorado las opiniones de organizaciones públicas y privadas sobre qué oportunidades y desafíos plantean la privacidad y la ética en el contexto de las tecnologías basadas en datos, proponemos el siguiente conjunto de recomendaciones a fin de ayudar a los legisladores en su esfuerzo por mejorar la gobernanza de datos:

Predicar con el ejemplo en materia de gobernanza de datos

Los responsables de formulación de políticas pueden sentar las bases de la buena gobernanza de datos si implementan la privacidad desde el diseño en los servicios públicos que prestan, optan por el código abierto sistemáticamente y experimentan con modelos emergentes de gobernanza de datos.

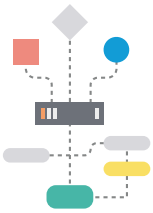
2 Impulsar la rendición de cuentas y una reforma regulatoria que lleve a la práctica los principios éticos

Se necesitan acciones concretas, más allá de compromisos, que garanticen que la recopilación, el uso y la gobernanza de datos en los sectores público y privado respondan a principios éticos.

3 Adoptar un enfoque inclusivo y transparente de gobernanza de datos más allá de las falacias del consentimiento y la transparencia

Los responsables de formulación de políticas pueden abordar la falta de inclusión y transparencia mejorando la alfabetización digital y promoviendo la diversidad en el sector tecnológico.

Glosario

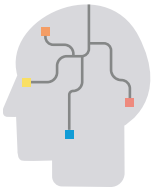


Algoritmo

Un algoritmo es un requisito inequívoco de un proceso que describe cómo resolver un tipo de problema; es capaz de realizar cálculos, procesar datos y automatizar el razonamiento.[1]

Ética de datos

La ética de los datos es la rama de la ética que estudia los problemas relacionados con el uso de datos (por ejemplo, generación, grabación, mantenimiento, procesamiento, difusión, intercambio), los algoritmos (por ejemplo, inteligencia artificial, agentes artificiales, aprendizaje automático y robots) y las prácticas correspondientes (por ejemplo, innovación responsable, programación, piratería y códigos profesionales) desde un punto de vista ético a fin de formular y promover soluciones éticamente apropiadas (por ejemplo, buena conducta o valores éticos).[2]



Inteligencia artificial (IA)

En su forma más básica, la inteligencia artificial es un sistema que toma decisiones de manera autónoma. La IA es una rama de la informática que programa ordenadores para que realicen tareas que normalmente requieren inteligencia humana, por ejemplo aprendizaje, razonamiento, resolución de problemas, comprensión del lenguaje y percepción de una situación o entorno. [3]

Privacidad

El derecho a la privacidad significa que cada persona tiene el derecho de decidir si comparte o no información sobre su vida privada, sus hábitos, actos y relaciones con los demás. [4] Existen cuatro grandes áreas de privacidad que destacan en el debate sobre la protección de datos y las leyes y prácticas de privacidad: la privacidad de la información, del cuerpo, del territorio y de las comunicaciones.[5] El pilar fundamental de la privacidad de la información es el derecho y la capacidad de los interesados de proteger sus datos personales frente a terceros.[6]

[1] Figure-eight.com 2019

[2] Floridi y Taddeo 2016

[3] Webb et al. 2019

[4] Warren y Brandeis 1890

[5] Iapp.org 2019

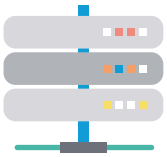
[6] Schermer 2011

Privacidad desde el diseño

"Privacidad desde el diseño" (*Privacy by Design*, en inglés) es una idea desarrollada por Ann Cavoukian en la década de 1990 y que aborda los efectos sistémicos y el constante crecimiento de las tecnologías de la información y la comunicación, las prácticas comerciales y los sistemas de datos en red a gran escala.[7]

Reglamento general de protección de datos (RGPD)

El Reglamento General de Protección de Datos sustituyó a la Directiva de protección de datos en 2018. El objetivo del RGPD es facilitar un conjunto de reglas de protección de datos a todos los Estados miembros de la Unión Europea y el Espacio Económico Europeo (EEE).[8]



Sistemas automatizados de toma de decisiones (ADMS)

Procedimientos o procesos que recopilan y analizan datos, interpretan los resultados de los análisis (según un modelo de interpretación definido por el ser humano) y actúan automáticamente en función de esa interpretación (sin intervención ni participación humana). Las decisiones pueden basarse en datos reales así como en perfiles creados digitalmente o en datos inferidos. Aunque los ADMS han demostrado ser extremadamente eficientes en la mejora del flujo de datos e información, su componente ético depende de los datos suministrados.

[7] Cavoukian 2019

[8] Iapp.org 2019

Transparencia

En el campo de la ética de la información, la transparencia se suele definir como la disponibilidad de la información, las condiciones de accesibilidad y la manera en que la información puede facilitar la toma de decisiones de los usuarios.[9]

Vendedores de datos

Entidades que recopilan, agregan y venden datos personales, derivados e inferencias obtenidos de fuentes públicas y privadas diversas.[10]

Violación de datos

Obtención no autorizada de datos informáticos que pone en riesgo la seguridad, la confidencialidad o la integridad de la información personal almacenada por un recopilador de datos.[11]

[9] Turilli y Floridi 2009

[10] Nytimes.com 2019

[11] Nytimes.com 2019

Introducción

Acerca de este informe

Las tecnologías basadas en datos nos prometen servicios más eficientes y una mejor calidad de vida, pero eso plantea una serie de inquietudes sobre las prácticas éticas de las entidades públicas y privadas a las que proporcionamos libremente nuestros datos todos los días. Este informe identifica desafíos comunes, oportunidades e imagina posibles escenarios dentro del panorama general de la ética de datos y señala caminos alternativos a través del debate continuo y conjunto, centrado en una visión del futuro digital en el que la sociedad pueda beneficiarse de las tecnologías basadas en datos a la vez que mitiga sus efectos perniciosos.

Nuestro objetivo final es dar a conocer a los responsables de formulación de políticas (cualquier persona que trabaje en gobiernos de todo el mundo y se encargue de establecer normas, marcos de gobierno y reglamentos que converjan con las tecnologías basadas en datos) medidas factibles que pueden implementarse ahora para construir sociedades digitales más inclusivas y equitativas.

Destinatarios

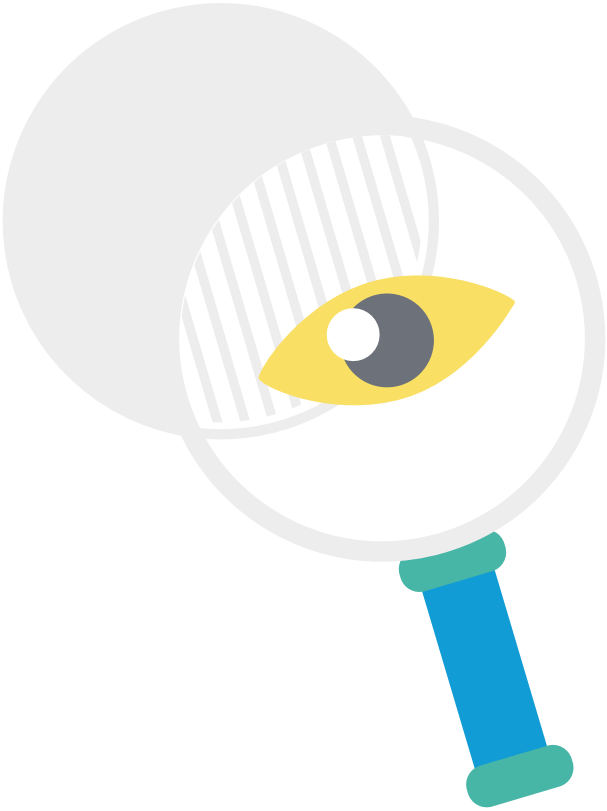
Los motivos éticos para proteger los datos personales, entre ellos evitar daños, impedir la explotación en los mercados de datos y prevenir la desigualdad y la discriminación derivadas del uso indebido de los datos, trasladan a los gobiernos y los responsables de formulación de políticas la necesidad de establecer leyes y reglamentos adecuados. Por ese motivo, nuestra investigación va dirigida a las personas y entidades que pueden provocar un cambio en las políticas.

Más allá de informar a los responsables de formulación de políticas sobre los desafíos y las oportunidades que conlleva transformar las sociedades mediante el despliegue de tecnologías basadas en datos, nuestro objetivo es influir en los actuales esfuerzos de gobernanza de datos iniciados por las entidades públicas y privadas, de manera que la economía digital de hoy y del mañana nos beneficie a todos.

Alcance

A medida que las tecnologías basadas en datos se generalizan en las infraestructuras de negocio y gobierno críticas para la sociedad, acaban afectando directamente a nuestro futuro social, cultural y económico. Por esta razón, nuestro enfoque se basa en cómo garantizar que los datos se utilicen para tomar decisiones éticas que respeten la privacidad de las personas y los grupos sociales, especialmente aquellos en riesgo de exclusión.[12]

Como no existe un modelo único para abordar los problemas de ética de los datos, nos hacemos eco de los expertos en la materia que han abogado por un «enfoque específico del sector» de las cuestiones de ética de datos.[13] En su vocación de globalidad, este informe también recala en el contexto transregional de Europa, Latinoamérica y África para seguir abordando la investigación con casos prácticos de todo el mundo. De esta manera, las conclusiones y recomendaciones que se alcancen podrán ser de aplicación general.



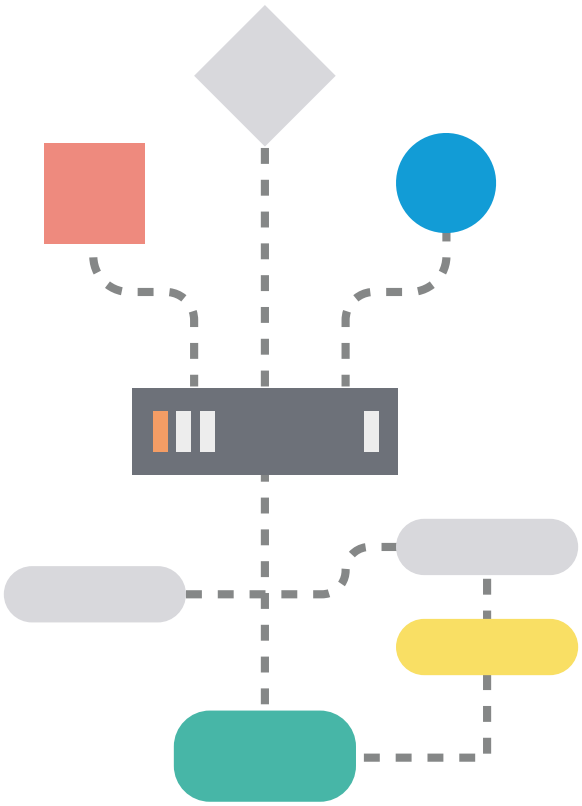
[12] Reloj de algoritmo 2018

[13] Whittaker et al. 2018

Estructura

Este informe presenta las ideas y recomendaciones a las que el programa Digital Future Society ha llegado a través de una combinación de investigación documental y consulta con la comunidad de expertos, líderes, organizaciones de la sociedad civil y responsables de formulación de políticas con experiencia en la implementación de la gobernanza de datos.

El primer capítulo define el concepto de ética de datos y hace un seguimiento de su evolución en los últimos años. La sección 2 se centra en las oportunidades y los desafíos a los que se enfrentan las organizaciones públicas y privadas a la hora de garantizar que la recopilación, el uso y la gobernanza de datos resulten éticos. En la sección 3 presentamos el concepto de diseño de futuros, basado en el análisis de las principales incertezas que afectarán a nuestras sociedades en los próximos años. A partir del análisis de los capítulos anteriores, la sección 4 comparte y expone recomendaciones esenciales para que los responsables de formulación de políticas mejoren y pongan en funcionamiento estructuras de gobernanza de datos éticos que centren sus esfuerzos en la transparencia, la responsabilidad y la educación.



1

Seguimiento de la evolución de la ética de datos

¿Qué es la ética de los datos?

En los últimos años, el debate sobre las políticas públicas relativas a la recopilación y el uso de información personal por parte de terceros se ha centrado básicamente en cuestiones de privacidad. Si bien se ha trabajado mucho en la regulación de la privacidad, es importante incorporar la ética de los datos al discurso de las políticas públicas, especialmente en el contexto de tecnologías basadas en datos como la inteligencia artificial, con el fin de aclarar y abordar el impacto del uso de datos por parte de terceros que está ausente del debate sobre la privacidad. Esto incluye el potencial de discriminación, la toma de decisiones sesgada, así como la agravación de los riesgos para la equidad, la igualdad y el respeto de las garantías procesales.[14]

La ética de los datos alude a la rama de la ética que estudia los problemas éticos que plantea el uso de los datos (por ejemplo, generación, grabación, mantenimiento, procesamiento, difusión, uso compartido), los algoritmos (por ejemplo, inteligencia artificial, agentes artificiales, aprendizaje automático y robots) y las prácticas correspondientes (innovación responsable, programación, piratería y códigos profesionales), a fin de formular y fomentar soluciones, conductas o valores éticamente correctos y aceptables.[15]

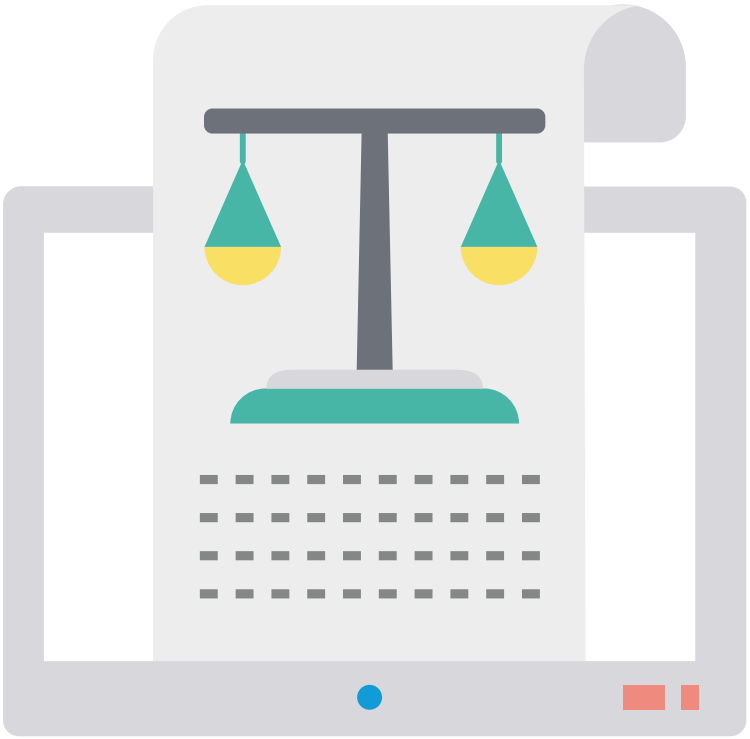
La ética de los datos guarda relación con cuestiones como la posible reidentificación de personas a través de grandes conjuntos de datos, la privacidad grupal y el riesgo de discriminación. La ética de los algoritmos aborda los numerosos problemas que surgen del uso de sistemas cada vez más complejos y automatizados, desde el establecimiento de objetivos de un sistema hasta su desarrollo y la selección de los datos que permiten al sistema aprender. La ética de las prácticas analiza cuestiones relacionadas con la responsabilidad de las organizaciones y los profesionales de los datos, por ejemplo expertos en datos, investigadores y programadores, que determinan los parámetros operativos de los algoritmos y cómo obtienen los datos que les permiten aprender.

[14] Informe «Building Ethics into Privacy Frameworks for Big Data and AI», 2018

[15] Floridi y Taddeo 2016

[16] Müller-Eiselt 2018

Estas tres áreas (datos, algoritmos y prácticas) están profundamente entrelazadas y pueden considerarse los tres ejes que definen el espacio conceptual con el que esquematizar los problemas éticos relacionados con la privacidad. Por ejemplo, un algoritmo utilizado en un contexto de auxilio en situaciones de desastre, por ejemplo para poner en contacto a las personas perdidas con sus familias, podría crear, por un lado, un conflicto entre los intereses individuales de privacidad, reflejado en los principios de limitación de finalidad y minimización de datos y, por otro, un conflicto entre los intereses generales de la sociedad, derivado de la predicción de resultados basados en patrones observados. La ética de datos es una parte central de la reconciliación entre, por un lado, la privacidad individual, y por otro, el beneficio social y colectivo derivado del uso compartido de datos.[18]



[17] Floridi y Taddeo 2016

[18] Informe «Building Ethics into Privacy Frameworks for Big Data and AI», 2018

Mapeo de la situación actual de la ética de datos

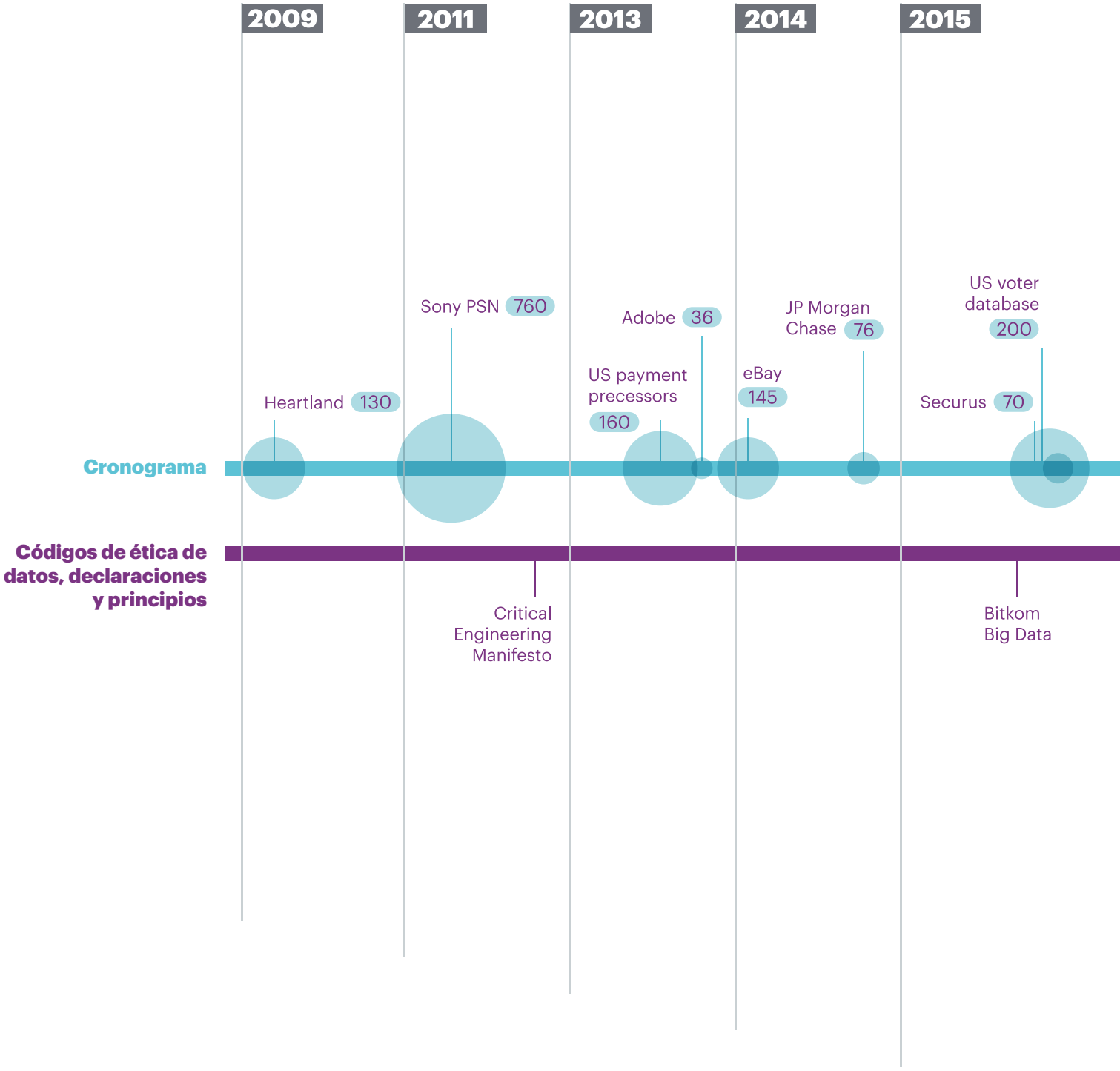
El panorama de la ética de datos es complejo. Surgen muchos desafíos al tratar de definirla y aplicarla, especialmente cuando entran en juego tecnologías digitales como la inteligencia artificial. Al mismo tiempo, los grupos de expertos han destacado que las pautas éticas y los códigos de conducta llevan presentes desde mucho tiempo en sectores como medicina, las finanzas y la biotecnología, además del mundo académico.

Los responsables de protección de datos, las juntas de revisión institucional y los equipos de validación empiezan a estar presentes en institutos de investigación e incluso en organizaciones privadas que innovan con *big data* e inteligencia artificial, por ejemplo la banca comercial. En las ciudades, las nuevas iniciativas de transparencia y los procesos participativos basados en "datos abiertos" (open data en inglés) se esfuerzan por encontrar un equilibrio entre la privacidad de los ciudadanos y la materialización de las ventajas que ofrecen los procesos de toma de decisiones digitales. Las universidades de todo el mundo han implementado políticas abiertas de ciencia e innovación, mientras que los comités de ética y otros organismos trabajan para garantizar que la investigación sea replicable, transparente y respetuosa con la privacidad de los sujetos. Los grupos de investigación y los programas educativos son cada vez más interdisciplinarios, con cursos de ciencias e ingeniería que incluyen clases sobre ética. La comunidad de investigadores científicos es otro actor clave en el contexto de la ética de datos y está impulsando un proceso de sensibilización y cambio de prácticas, especialmente en el sector emergente de la IA.

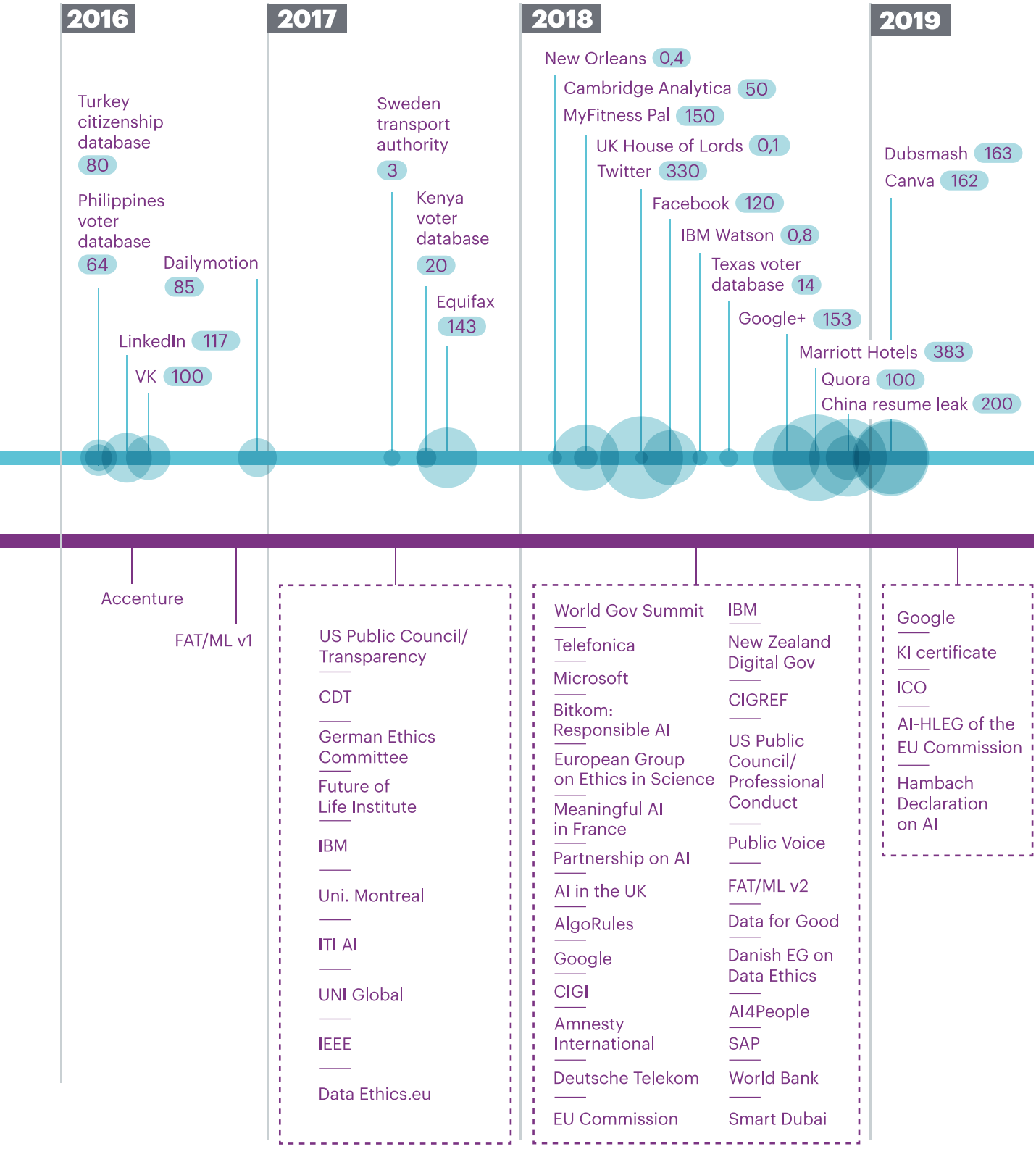
Sin embargo, las anteriores prácticas no son la norma en todos los sectores y resultan insuficientes dada la omnipresencia de los datos y los riesgos asociados al mal uso; además de otras consecuencias potencialmente negativas como la discriminación y el sesgo algorítmico.

Las violaciones de datos, la piratería y los escándalos de abuso de privacidad se han vuelto cada vez más habituales en todo el mundo, como demuestra el gráfico siguiente:

VIOLACIONES DE DATOS frente a CÓDIGOS DE ÉTICA DE DATOS

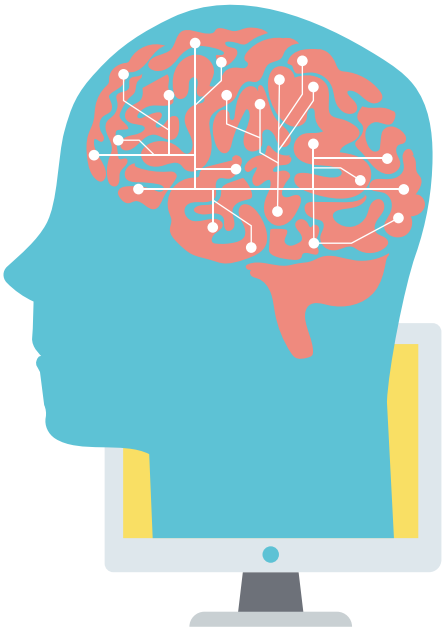


Fuente de las imágenes: Digital Future Society


2016
2017
2018
2019
Turkey citizenship database 80
Philippines voter database 64
Dailymotion 85
LinkedIn 117
VK 100
Sweden transport authority 3
Kenya voter database 20
Equifax 143
New Orleans 0,4
Cambridge Analytica 50
MyFitness Pal 150
UK House of Lords 0,1
Twitter 330
Facebook 120
IBM Watson 0,8
Texas voter database 14
Google+ 153
Marriott Hotels 383
Quora 100
China resume leak 200
Dubsmash 163
Canva 162
Accenture
FAT/ML v1
US Public Council/ Transparency
CDT
German Ethics Committee
Future of Life Institute
IBM
Uni. Montreal
ITI AI
UNI Global
IEEE
Data Ethics.eu
World Gov Summit
Telefonica
Microsoft
Bitkom: Responsible AI
European Group on Ethics in Science
Meaningful AI in France
Partnership on AI
AI in the UK
AlgoRules
Google
CIGI
Amnesty International
Deutsche Telekom
EU Commission
IBM
New Zealand Digital Gov
CIGREF
US Public Council/ Professional Conduct
Public Voice
FAT/ML v2
Data for Good
Danish EG on Data Ethics
AI4People
SAP
World Bank
Smart Dubai
Google
KI certificate
ICO
AI-HLEG of the EU Commission
Hambach Declaration on AI

Aplicación de la ética de los datos a la investigación de supercomputación

La supercomputación es el núcleo en el que se basa el desarrollo de la IA. Desde el aprendizaje profundo y las redes neuronales de aprendizaje hasta la integración de *big data* en redes masivas, las prácticas éticas de recopilación y procesamiento de datos resultan críticas en muchas de las actividades de investigación en el Barcelona Supercomputing Center (BSC). Por ejemplo, aunque el BSC no recopila datos, ha designado un comité ético externo que supervisa y aprueba todos los proyectos de investigación. El director científico del *High-Performance Artificial Intelligence Group*, Ulises Cortés, explica cómo se incorpora la ética en el BSC: "Se consulta a un comité ético externo que evalúa todos los experimentos que incluyen datos personales y/o confidenciales, lo que garantiza el cumplimiento del código ético que predomina en el entorno académico y científico".



Además de asegurar el cumplimiento de las normas, el BSC también ha adoptado medidas para transformar los principios éticos en acciones concretas a través de su participación en el proyecto europeo de inteligencia artificial AI4EU. El BSC se encarga en estos momentos de supervisar la puesta en práctica de las directrices de integridad de la IA en varias entidades privadas y públicas. Además del proyecto AI4EU, el BSC también coordina actividades para promover la aplicación de las directrices y contribuye a la creación de un observatorio para estudiar el uso ético de la IA en Europa.

En segundo lugar, las prácticas de datos son cada vez más sofisticadas, encubiertas e invasivas. Esta tendencia, que ocasiona la pérdida de privacidad, la resume a continuación Cory Doctorow, autor de ciencia ficción, profesor de informática y activista de la tecnología:

> **"[...]las plataformas aprovechan tanto los datos de comportamiento de sus usuarios como la capacidad de crear una dependencia de su propio producto para impulsar el crecimiento y las ganancias. Los clientes de estos sistemas se tratan como si hubieran suscrito un contrato negociado [...] para intercambiar privacidad por servicio o exclusividad de proveedor por algún tipo de ayuda o facilidad. [Los recopiladores de datos afirman] que sus clientes negociaron un acuerdo en el que cedieron su información personal a cambio de ser saqueados y vendidos, o su libertad de adquirir servicios y recambios en el mercado abierto. Pero es obvio que tal negociación no ha tenido lugar. Tu navegador es una sanguijuela que, de forma invisible y silenciosa, chupa la sangre de tu información personal mientras te mueves por la web."**[19]

Paralelamente, en Europa se promulgó un nuevo marco regulatorio de protección de datos que fomenta el desarrollo de una infraestructura de privacidad desde el diseño.[20] Aprobado en 2018, el Reglamento General Europeo de Protección de Datos (RGPD) proporciona un marco que regula la privacidad de la información, el consentimiento, la transparencia y la explicabilidad, el derecho al olvido o a ser borrado, la portabilidad de los datos y la privacidad desde el diseño. Hasta la fecha, el RGPD ha servido de modelo a muchas organizaciones y gobiernos en materia de gobernanza y privacidad de datos, lo que sitúa a Europa a la vanguardia del diseño digital ético. Se están desarrollando o revisando marcos similares en todo el mundo, y la mayoría de ellos comparten principios básicos de privacidad, como la transparencia, la elección efectiva, la responsabilidad y la seguridad. Algunos ejemplos son Brunei (2015)[21] China[22] y Kenia (2018)[23] y Tailandia (2019).[24]

Más allá de la evolución de los marcos legales y reglamentarios de protección de datos y privacidad, solo en los últimos dos años hemos observado un número creciente de principios, compromisos voluntarios y marcos dirigidos al uso ético de los datos, sobre todo en lo relativo a la IA.[25]

En resumen, la cuestión de la ética de los datos ha dejado de circunscribirse al mundo académico y los dominios de investigación clínica y ha entrado en la esfera pública, impulsada por prácticas cuestionables, hasta generar una mayor concienciación sobre la privacidad y la ética de los datos. A pesar de esa mayor concienciación, quedan por resolver muchos matices de los desafíos y las oportunidades que se plantean antes de que los sistemas basados en el uso ético de datos se generalicen. Sobre ellos hablamos en la siguiente sección, con el fin de proponer recomendaciones útiles que mejoren las políticas de gobernanza de datos.

[19] Doctorow 2019
[20] Ver Anexo II
[21] Salleh Rahaman 2015
[22] Liao 2018
[23] Política de privacidad y protección de datos 2018
[24] Inside Privacy 2019
[25] Ver Anexo I

2

Desafíos y oportunidades

Sopesando las complejidades de la gobernanza de datos

El rápido crecimiento de la datificación y la digitalización en casi todos los aspectos de la sociedad moderna hace que los ciudadanos sean más vulnerables al uso incorrecto de los datos, por ejemplo al sesgo algorítmico y sistemático integrado en tecnologías digitales que están diseñadas, conscientemente o no, para discriminar a ciertos grupos sociales, de género y étnicos o incluso a violaciones de datos personales a través de plataformas en línea. Si bien la rendición de cuentas y la transparencia ganan las agendas de las instituciones públicas y privadas por igual, quedan por resolver los siguientes desafíos antes de que las tecnologías basadas en datos se puedan implementar de manera segura y ética.

Desafíos de la era de los datos

Los datos pueden ser una ventaja, pero también plantean riesgos. Si bien existe un debate creciente que busca acordar normas, funciones, derechos y responsabilidades globales que hagan frente a esos riesgos, las tensiones y los enfrentamientos entre legislaciones y valores culturales se acentúan, como se ilustra en los siguientes desafíos.

Sesgo algorítmico

Los líderes empresariales, los gobiernos y los investigadores coinciden en el potencial de la IA y otras tecnologías basadas en datos para mejorar nuestras vidas. Pero también están de acuerdo en que esos sistemas tienen un problema: el sesgo y el riesgo de discriminación.[26] Los algoritmos, por naturaleza, están cargados de valores que reflejan la vida y la procedencia de los ingenieros que los crearon, generalmente hombres blancos de países con altos ingresos.[27] Más tarde los configuran usuarios con deseos y moralidades que anteponen ciertos valores e intereses a otros. Es más difícil evitar la incorporación involuntaria de sesgo en los algoritmos cuando en los equipos de desarrolladores no existe diversidad ni interdisciplinariedad suficientes para modelar diferentes realidades y complejidades al generar decisiones automatizadas.

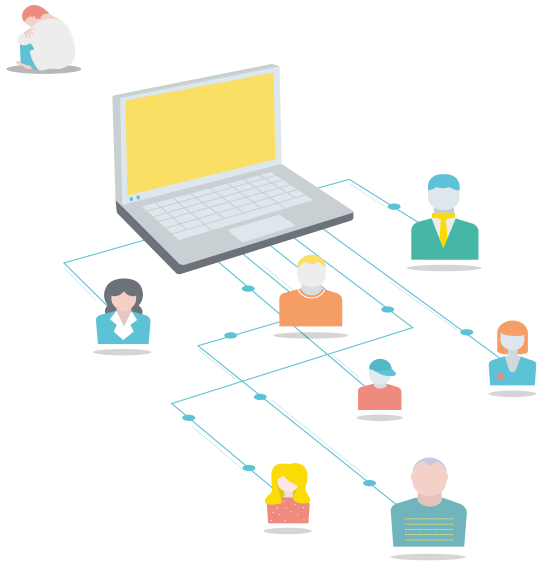
[26] Powles y Nissenbaum 2018

[27] Vincent 2019

Tomemos, por ejemplo, el caso del servicio de entrega en el mismo día de Amazon, donde el sector público tuvo que movilizarse para garantizar que las personas de todos los vecindarios tuvieran la misma opción de entrega en el mismo día, no solo los códigos postales vinculados a rentas más altas.[28]

El diseño de algoritmos no solo puede generar sesgo, sino que la transferencia de servicios y la aparición de nuevos productos digitales también pueden terminar reproduciendo o agravando las desigualdades existentes. Por ejemplo, un nuevo estudio de los algoritmos de reconocimiento de objetos más utilizados descubrió que cometían un 10% más de errores cuando los algoritmos debían identificar artículos de un hogar con ingresos mensuales más bajos.[29] Además, esos algoritmos eran entre un 15 y un 20% más efectivos reconociendo objetos del Reino Unido o Estados Unidos de Burkina Faso, Somalia o Nepal.[30]

> **"Todos los algoritmos están sesgados porque los propios datos están sesgados y los criterios utilizados en los algoritmos tienen una base cultural, por lo que el sesgo se está cronificando. O eso, o faltan datos y se introducen variables proxy que también pueden generar sesgo".** [31]
> **- Cathy O'Neil, matemática y autora**



Concentraciones de datos

Muchas de las principales empresas del mundo dependen de los datos para impulsar sus modelos de negocio. Alphabet, Amazon, Apple, Facebook y Microsoft en Estados Unidos y Alibaba, Baidu y Tencent en China disfrutan de importantes ventajas competitivas al poseer conjuntos de datos masivos. Sin embargo, la concentración de datos en un número limitado de empresas plantea un desafío, ya que limita las posibilidades de extracción de valor público de los datos. Además, la falta de competencia en el mercado ofrece a los consumidores pocas opciones alternativas para la protección de la privacidad, y es probable que no aparezca ninguna.[32]

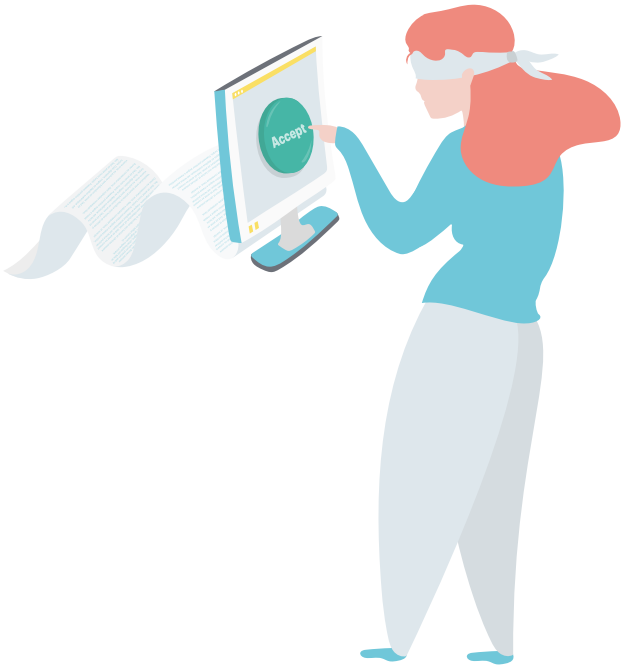
[28] Ingold y Soper 2016
[29] Vincent 2019
[30] Ibid.
[31] VPRO 2018
[32] Doctorow 2019

El uso de datos éticos conlleva múltiples costes

Al no existir un mercado para el uso ético de datos, los gobiernos se enfrentan a desafíos al crear condiciones en las que el comportamiento ético no afecte a la competitividad de las grandes y pequeñas empresas. Pensemos en los sistemas de IA que dependen de datos etiquetados en el sector de innovaciones en la tecnología de la salud. Aunque el proceso de recopilación de datos éticos se entiende y está legalmente establecido, las tareas de etiquetado corren el riesgo de afectar desproporcionadamente a grupos vulnerables. Sin embargo, el uso de etiquetas de origen ético lleva asociado un considerable coste. Si bien están surgiendo proveedores éticos, aún no son competitivos, ya que operan principalmente como organizaciones sin ánimo de lucro en el ámbito de la educación y otros programas sociales. A medida que evoluciona el desafío de la recopilación y el etiquetado ético de datos, la aparición de grandes "granjas de datos" (*data farms* en inglés) en Asia y África plantea muchos interrogantes sobre las condiciones laborales de estos nuevos trabajos. "Debemos tener cuidado para evitar crear una nueva generación de fábricas de explotación", advierte un experto.

Superar la falta de alfabetización de datos

Aunque la concienciación sobre las consecuencias de compartir datos con organizaciones públicas y privadas crece, la mayoría sigue sin comprender los posibles usos secundarios de los datos. Por ejemplo, las justificaciones para recopilar y vender datos, también conocidas como políticas de privacidad, tienden a ser excesivamente detalladas y plagadas de tecnicismos, lo que hace que sean casi imposibles de entender para el usuario medio de Internet. El mercado de datos en el que se ha convertido Internet está impulsado en gran medida por ciudadanos que aceptan pero no entienden completamente las políticas de privacidad. Los expertos del grupo de trabajo señalaron un importante desafío a la hora de impulsar la alfabetización de datos: garantizar que las personas y las organizaciones no sólo entiendan las consecuencias de la recopilación y el uso de datos, sino también su valor.



Esquivar la falacia de la transparencia

A medida que la IA se vuelva más sofisticada, será más difícil de explicar de una manera comprensible. Con la complejidad de los algoritmos en aumento, el derecho a una mayor transparencia puede volverse contraproducente si los ciudadanos carecen de conocimientos suficientes sobre datos para ejercer dichos derechos. Es un problema al que no sólo se enfrentan los ciudadanos; también los programadores tienen dificultades para comprender o explicar las decisiones tomadas por algunas redes neuronales. Como explica un miembro del grupo de trabajo:

> **"Confiar en que los derechos individuales de explicación sea la manera en que el usuario tome el control de los sistemas algorítmicos implica el riesgo de crear una falacia de transparencia. Las personas no están empoderadas para aprovechar el tipo de explicaciones algorítmicas que probablemente se les ofrezca; la mayoría carece del tiempo, los recursos y la experiencia necesarios para ejercer efectivamente esos derechos individuales".**[33]

Seguridad y mayor riesgo de violaciones de datos

Los ataques cibernéticos y las amenazas de "fraude masivo de datos" se encuentran periódicamente entre los cinco principales riesgos mundiales enumerados por el Foro Económico Mundial (FEM).[34] Según la última encuesta anual del FEM, se espera que el robo de dinero y/o datos, así como la afectación de las operaciones y/o las infraestructuras, sigan aumentando año tras año.[35] Es probable que el avance de la inteligencia artificial aumente la sofisticación de los ataques cibernéticos y dificulte aún más predecirlos.

Establecer la obligación de rendir cuentas

Hay quien argumenta que los algoritmos basados en el aprendizaje automático deberían considerarse agentes éticos con cierto grado de responsabilidad.[36] Los modelos tradicionales de rendición de cuentas tienden a fallar dado que, en la mayoría de los casos, nadie controla lo suficiente un sistema automatizado de toma de decisiones como para asumir la responsabilidad de sus decisiones. La implementación de mecanismos factibles de rendición de cuentas que aseguren que las decisiones de esos sistemas sean justas y no discriminen sigue siendo un enorme desafío.

Gemelos digitales y la erosión de la autonomía moral

La autonomía moral alude a la capacidad de una persona de exponer su propia identidad a los demás y de resistir a los intentos de estereotipar sus elecciones o su biografía. Un ser humano es moralmente autónomo cuando es el autor de su propio recorrido moral.[37] En otras palabras, cuando podemos elegir cómo queremos ser y luchar por esa identidad tenemos la capacidad de resistir las presiones externas que intentan encasillarnos.

---

[33] Edwards y Veale 2017

[34] La era de la interdependencia digital 2019

[35] Informe de riesgos globales 2019

[36] Mittelstadt et al. 2016

[37] van den Hoven 2008

Sin embargo, este esfuerzo por conformar la propia identidad basada en valores morales se ve amenazado cuando los recopiladores de datos ya nos han clasificado en función de los datos recogidos sobre nosotros, lo que a veces se llama “gemelo digital” (digital twin, en inglés)..

El caso de Sorine

Corre el año 2030 y Sorine, de camino a casa desde su nuevo trabajo de diseñadora, busca en el bolso un ibuprofeno. Sorine se toma el analgésico y se sienta en el tranvía sin conductor. «Ya está aquí otra vez», piensa, mientras inicia sesión con Facebook en su aplicación de seguimiento del período y escribe algunos síntomas. Al llegar a casa revisa el correo electrónico. Sorprendida de ver el nombre de la aplicación de seguimiento del período que estaba usando, abre el mensaje y descubre que alguien ha entrado en su cuenta. Sorprendida y molesta, Sorine elimina rápidamente la aplicación del teléfono y se decide a encontrar un programa más seguro de seguimiento de periodo. Semanas después, Sorine todavía no puede estar segura de que sus datos personales de salud no se vendan a las compañías de seguros. Ya se han vendido a los comerciantes, eso lo sabe porque los anuncios de pruebas de embarazo siguen apareciendo en los vídeos de YouTube y cuando navega por Instagram. ¿Y si su empresa de alguna manera se enterara... estaría en riesgo su nuevo trabajo?

De hecho, los datos sobre el ciclo menstrual de Sorine no son lo que persiguen esas empresas; sino los «residuos digitales» que deja cuando lee artículos o mira vídeos, publica sobre su nuevo trabajo o incluso busca recetas. Estos metadatos se utilizan para hacer inferencias que, combinadas, crean un perfil de Sorine, su gemelo digital, cuyo comportamiento potencial se rastrea, analiza y etiqueta cuidadosamente. Las empresas que apuestan por cómo se comportará la Sorine digital en esos mercados se están beneficiando de ella sin su conocimiento o consentimiento. Esos son los usos secundarios de los metadatos sobre los que Sorine, y el resto de los que utilizamos aplicaciones y plataformas y servicios gratuitos en línea, no tenemos control.

Modelos de gobernanza de datos problemáticos

Los modelos de gobernanza de datos basados en el consentimiento y en la propiedad no consiguen proteger al público contra ciertas violaciones de la privacidad ni contra la recopilación y el uso poco ético de los datos personales. Los expertos del grupo de trabajo sugieren que incluso la histórica normativa sobre la privacidad que representa el RGPD no llega a garantizar el uso ético de los datos en un entorno dónde los sistemas impulsados algorítmicamente son omnipresentes. Señalan que nuestra concepción colectiva del consentimiento parece haber pasado de la libre determinación de proporcionar información a la mera legitimación de la extracción de datos personales en la mayoría de los casos.

> **"Tanto los usuarios como los proveedores de tecnología parecen tratar el consentimiento como un derecho concedido innecesariamente", observa un miembro del grupo de trabajo. "Más preocupante es la posibilidad de volver a identificar a las personas a partir de grandes conjuntos de datos. El desafío es garantizar que las entidades públicas y privadas entiendan y respeten el derecho al olvido."**

Del mismo modo, el concepto de la titularidad, pregonada como la solución a los problemas de gobernanza de datos, no es fácil de aplicar a los datos y no aborda cuestiones importantes sobre el acceso, el uso y el impacto de los resultados, especialmente en el contexto de tecnologías como los sistemas automatizados de toma de decisiones.

Finalmente, el derecho a la portabilidad, en el que los interesados tienen derecho a recibir sus datos en un formato legible por máquina, es problemático. Si bien obtener los datos puede ser fácil, usarlos para obtener servicios similares de otro proveedor podría ser imposible. Por lo tanto, la portabilidad es un sustituto inadecuado de la capacidad de migrar a un servicio diferente para administrar los datos, como lo demuestra el caso en el que la colección de fotos meticulosamente organizada de un usuario de Flickr solo se podía descargar en conjuntos aleatorios de archivos sin etiquetar.[38]

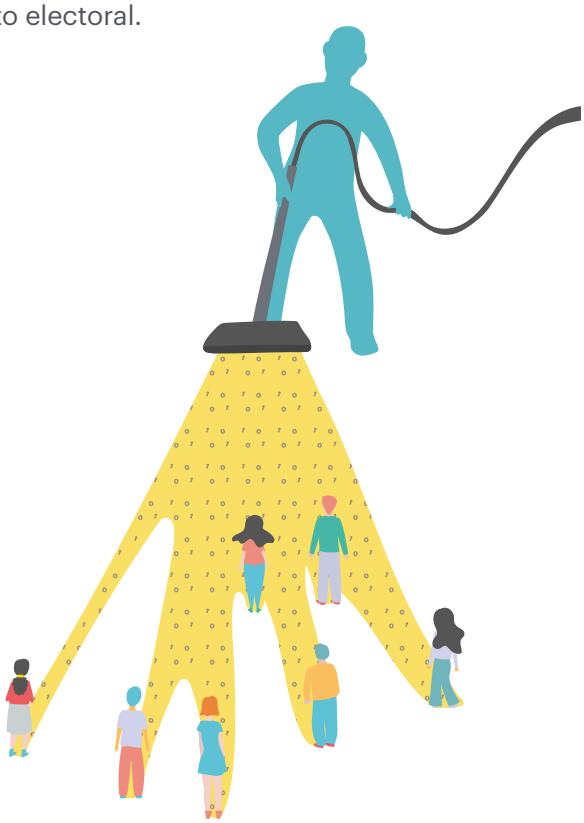
El desafío de la gobernanza de datos global

El hecho de que las actitudes hacia la privacidad, los enfoques de gobernanza de datos y las estrategias de desarrollo tecnológico difieran ampliamente de un lugar a otro plantea un desafío para el desarrollo de mecanismos transnacionales de gobernanza de datos. Por ejemplo, mientras que el plan de IA de China se centra en impulsar la competitividad internacional de su sector privado, Estados Unidos permite que las fuerzas del mercado definan su enfoque de gobernanza de datos y el sector público apoya la investigación y el emprendimiento. Por su parte, la UE adopta la posición de que cualquier desarrollo de IA debe situar a los humanos en el centro y se basa en la ética de los datos como principio rector tanto del sector público como del privado. Otros países aún tienen que implementar mecanismos de gobernanza de datos, lo que puede plantear nuevos tipos de desafíos.

[38] Furseth 2019

Demasiada información: El caso del registro de votantes de Kenia

La legislación de Kenia establece que el registro de votantes debe publicarse antes de las elecciones. En un intento por mejorar la eficiencia y reducir de antemano los costes de las elecciones de 2017, el organismo de gestión electoral de Kenia (IEBC) publicó el registro en línea. Los datos publicados incluían el número de documento de identidad nacional de los votantes, la fecha de nacimiento y el género, junto con el nombre completo y el distrito electoral.



La base de datos se podía consultar con el número del documento de identidad o tras enviar un número de identificación nacional a un número de SMS concreto.

La Kenya ICT Action Network (KICTANet) observó con preocupación que el portal en línea revelaba información innecesaria al publicar el registro de votantes. La exposición de los números de identificación nacionales era especialmente preocupante, ya que es el mismo número que va asociado a numerosos registros, gubernamentales y privados. Se podría usar para vincular los datos de las personas mediante tecnologías de minería de bases de datos relacionales. Además, las escasas medidas de seguridad del portal en línea hacían que fuera vulnerable al riesgo de la minería de datos automatizada.

En uno de los foros en línea de KICTANet, los usuarios compartieron sus experiencias al consultar el portal de registro de votantes de IEBC. Muchos explicaron que pudieron consultar números aleatorios. Otros mensajes afirmaban que se podía enviar números de documentos de identidad al número de SMS infinitas veces.

Esto abrió el debate de cómo cumplir el requisito legal de publicar el registro de votantes sin poner en riesgo los datos personales de los votantes. Se invitó a un representante de IEBC al foro en línea, donde explicó los motivos para publicar el registro y dio respuesta los problemas planteados por el público, entre ellos la presencia de votantes muertos, los números de identificación mezclados y los registros múltiples, ninguno de los cuales había previsto el IEBC.

KICTANet hizo varias recomendaciones para que se retirara información que no era necesaria para cumplir con el requisito de publicación, por ejemplo la fecha de nacimiento y el género. La publicación del número de identidad nacional fue objeto de debate. Mientras que algunos usuarios del foro expresaron su preocupación por el uso de la información de identificación para relacionar los datos de los votantes con otras bases de datos, otros pensaron que era la forma más segura para que el público identificara imprecisiones en el registro de votantes. Como alternativa, se sugirió utilizar un número identificativo de votante.

Para evitar la minería automatizada de datos, los usuarios del foro KICTANet recomendaron el uso de "disuasores de robots" (robot deterrents en inglés) como captcha. El IEBC adoptó de inmediato la función de disuasión de robots. En cuestión de días, también limitaron la información personal visible al consultar la base de datos. Meses después de las elecciones, los informes indicaron que los actores políticos habían obtenido datos del registro de votantes y los habían utilizado para enviar mensajes personalizados a los votantes, en algunos casos manipulándolos. Los informes también señalaron que los partidos políticos obtuvieron el registro de votantes completo.

KICTANet ha investigado las políticas y propuesto un marco integral de protección de datos en Kenia. El trabajo realizado incluyó una investigación sobre el estado de la protección de datos en Kenia y el compromiso con los comités parlamentarios sobre las TIC. La red KICTANet contribuyó decisivamente a dos proyectos de ley de protección de datos, cuyo estado somete a seguimiento. Aunque el IEBC finalmente mejoró sus prácticas de privacidad, fue una respuesta ad hoc a las preocupaciones por la privacidad de datos del registro de votantes que podrían haberse evitado si se hubiera establecido un marco integral de protección de datos.

El caso de Kenia ilustra el desafío que plantea la digitalización del sector público sin la evaluación previa del impacto sobre la privacidad asociado al despliegue de la tecnología. Sin embargo, también puede entenderse como una oportunidad para que las organizaciones de interés público defiendan mejores prácticas de privacidad, si las organizaciones del sector público se muestran abiertas a recibir críticas. Las entidades del sector público deben tener la voluntad política de comprometerse decisivamente con quienes realizan aportaciones.

La aplicación de la ética más allá del postureo ético

Como se muestra en el Anexo I, durante los últimos dos años ha surgido un gran número de códigos y principios éticos para el desarrollo y el uso de la IA, provenientes de entidades públicas y privadas, así como del tercer sector. Aunque es un paso prometedor, la mayoría de las declaraciones vienen en forma de comunicados (como "nos aseguraremos de que nuestros conjuntos de datos no estén sesgados") y carecen de recomendaciones viables, mecanismos de gobernanza y rendición de cuentas o ejemplos de cómo llevar a la práctica los principios éticos de una manera que respete los derechos humanos.

Como observó un miembro del grupo de trabajo, es algo comprensible dado que "no todos los derechos humanos pueden traducirse en derechos digitales y no todos los aspectos del mundo digital se ajustan a un marco de derechos humanos". Del mismo modo, los costes de infraestructura necesarios para asegurar el tratamiento ético de los datos (como pagar por alternativas a los gigantes de los datos) podrían ser prohibitivos para las organizaciones más pequeñas. La cuestión de cómo implementar una legislación de privacidad de primer nivel y pautas de datos éticos en las pymes y otras organizaciones con menos recursos es uno de los grandes retos sobre los que incide el programa Digital Future Society. Aun así, cuando las organizaciones, de cualquier tamaño, se comprometen a seguir pautas éticas sin indicar cómo las harán realidad, las declaraciones éticas corren el riesgo de ser tildadas de pura fachada o postureo ético.

Un segundo desafío que conlleva esta proliferación de principios éticos es la necesidad de una mayor coordinación o colaboración digital. La disgregación o atomización del esfuerzo dificulta, en la práctica, evaluar el alcance y la efectividad de los principios de ética de datos. Más allá de la regulación de la ética de los datos y de la privacidad digital, uno de los principales desafíos que hay que afrontar es la formación ética de los programadores y quienes diseñan sistemas de inteligencia artificial. Los datos recientes demuestran que los códigos de ética pueden tener un efecto irrisorio en el cambio de comportamiento, al menos entre los desarrolladores de software que son cruciales en el diseño y la puesta en marcha de sistemas automatizados de toma de decisiones.[39]

[39] McNamara et al. 2018

Oportunidades para un uso más responsable de los datos

Los datos, incluidos los datos personales, pueden tener muchos usos y resultados positivos. Que la toma de decisiones automatizada se esté convirtiendo en un elemento central de las tecnologías que utilizamos en nuestra vida diaria no es intrínsecamente negativo; cualquier persona que use un teléfono móvil, realice una transacción bancaria o reserve un vuelo se ha beneficiado de esas tecnologías. Del mismo modo, la sincronización de los semáforos en cualquier ciudad o la velocidad controlada de los trenes subterráneos requieren un sistema automatizado de toma de decisiones para funcionar sin problemas y con seguridad. Además de ventajas como la mayor eficiencia y los menores costes de los productos y servicios basados en sistemas impulsados por datos, existen maneras de garantizar que la recopilación, el uso y la gobernanza de los datos sean éticos y respeten la privacidad.

La ventaja competitiva de la privacidad

Según el informe Internet Trends de 2019, la privacidad se está convirtiendo en un argumento de venta cada vez más importante a medida que aumenta la demanda del consumidor de opciones de comunicación digital más seguras. A día de hoy, el 87% del tráfico global de la red está encriptado, en comparación con el 53% de hace tres años.[40] En los mercados en los que los consumidores suben progresivamente el listón y valoran cada vez más la privacidad, el grado de concienciación e implicación en cuestión de ética de datos de una empresa sirve de acicate para desarrollar productos y servicios éticos, a pesar de los costes potenciales.

Consenso en torno a la explicabilidad

Existe un creciente consenso global según el cual los sistemas inteligentes autónomos deben diseñarse para que sus decisiones puedan explicarse. En el caso de los llamados algoritmos de caja negra, puede que sean necesarias otras medidas de explicabilidad (trazabilidad, control, auditoría y comunicación transparente respecto a las capacidades del sistema), siempre que el sistema en su conjunto respete los derechos humanos fundamentales. Sin embargo, el grado de explicabilidad necesario depende, en gran medida, del contexto y de la gravedad de las consecuencias si los resultados son erróneos o inexactos.

[40] Molla 2019

Interoperabilidad

La interoperabilidad permite que los datos fluyan con fines comerciales, de investigación y gubernamentales y es un ingrediente esencial de la innovación. Según el Panel de Alto Nivel del Secretario General de las Naciones Unidas sobre Cooperación Digital, existe la posibilidad de poner en marcha proyectos de colaboración que examinen la interoperabilidad de datos, normas y sistemas de protección en todo el mundo.[41]

La interoperabilidad tiene el potencial de servir no solo para la cooperación en materia de datos, sino también de palanca competitiva que contrarreste la concentración de datos y permita a quienes accedan al mercado de datos asumir los efectos de red.[42] En países de bajos y medianos ingresos donde los recursos limitados dan fuerza a la idea de una digitalización que mejore la prestación de servicios públicos, es vital que las ciudades y otras entidades gubernamentales, a nivel nacional e internacional, compartan las lecciones y las mejoras. fAIr LAC es un ambicioso proyecto de Latinoamérica y el Caribe que busca aprovechar las ventajas de la IA a la vez que trata de disipar las reticencias de la sociedad hacia la automatización. Para el Banco Interamericano de Desarrollo, que lidera esta iniciativa, la oportunidad radica en la colaboración, manifestada a través de tres actividades principales: compartir modelos predictivos de políticas sociales, fortalecer el alcance del emprendimiento local y capacitar y desarrollar normas para que los sistemas de IA de la región sean interoperables.

[41] La era de la interdependencia digital 2019

[42] Doctorow 2019

Aparición de nuevos modelos y herramientas de gobernanza de datos

El debate sobre la gobernanza de datos se está desplazando hacia la noción de ecosistemas de instituciones que colaboran de acuerdo con diferentes condiciones de consentimiento, con una puesta al día del concepto de valor público y privado a fin de maximizar los beneficios públicos de los datos. Un ejemplo es la Plataforma de CGIAR para Big Data en la Agricultura, creada en 2017 por el Centro Internacional de Agricultura Tropical, con sede en Colombia, tras consultar a *stakeholders* de los sectores público, privado y sin ánimo de lucro.[43] La plataforma proporciona nuevas formas de compartir datos agrícolas y busca transformar la investigación y la innovación en seguridad alimentaria, sostenibilidad y cambio climático.[44] Otro ejemplo de modelo emergente de gobernanza de datos basado en un enfoque de ecosistema colaborativo es el de los *data trusts*.[45]

[43] La era de la interdependencia digital 2019

[44] Plataforma de CGAIR para Big Data en Agricultura 2019

[45] Mulgan y Straub 2019

Caso práctico:
El agrupamiento de derechos individuales de privacidad de los datos a través de *data trusts*

Los *data trusts* están ganando interés y aceptación como modelos de administración y gestión de datos que permiten a las entidades públicas y privadas aprovechar sus recursos compartidos. Es una idea prestada del sector de las finanzas y consiste en transferir las estructuras de gobernanza de fideicomisos que sirven para mantener recursos compartidos, por ejemplo terrenos públicos y fondos de pensiones, a la gobernanza de los datos.[46] Los *data trusts* son una oportunidad para equilibrar puntos de vista e incentivos en conflicto respecto al acceso a datos y facilitan la colaboración frente desafíos comunes, lo que permite crear nuevos productos y servicios. También pueden reducir los costes de intercambio de datos y crear nuevas oportunidades para las empresas que innovan con datos.[47]

Junto con el Open Data Institute, la Oficina de Inteligencia Artificial del Reino Unido e Innovate UK se encargan de pilotar un modelo de estructuras legales que permite la administración independiente de datos basado en los data trust en tres escenarios diferentes: datos del espacio urbano, datos de imagen y acústicos de las fronteras para combatir el comercio ilegal de animales salvajes y datos de ventas para reducir el desperdicio mundial de alimentos.[48] En cada caso existe un data trust que funciona como una entidad independiente que decide cómo usar y compartir datos para un propósito acordado. Para implementar estos proyectos piloto fueron necesarios la participación de las partes interesadas, un análisis jurídico, un estudio de la estructura jurídica necesaria, el diseño de un proceso de toma de decisiones, la evaluación de la arquitectura técnica que daría acceso a los datos a través de un data trust y un estudio de viabilidad. La experiencia muestra que no existe una estructura jurídica única que se adapte a todos los *data trusts* y que cada uno requiere un diseño y enfoque de toma de decisiones propios que se reflejen en su modelo jurídico.[49] El ritmo de los procesos de toma de decisiones, por ejemplo, será más rápido en *data trusts* de organizaciones privadas que en aquellos que administran datos de los sectores público y privado.

Aunque el deseo de seguir experimentando con este modelo de acceso e intercambio de datos crece, la definición del término data trust sigue abierta puesto que sus características no se corresponden exactamente con las de su equivalente financiero. Por esta razón, se aconseja a las entidades públicas que consideren emplear otro término como "cooperativa de datos" (*data cooperatives* en inglés) o "contrato de intercambio de datos" (*data sharing contract* en inglés). Los gobiernos y otros actores interesados en mejorar sus propios modelos de gobernanza de datos pueden acercarse a la creciente constelación de organizaciones de todo el mundo que trabajan abiertamente para compartir experiencias y aprendizajes, por ejemplo el Governance Laboratory, la Royal Society, la British Academy, la Data Stewards Network, Element AI, Nesta y el Centre for International Governance Innovation.

[46] Wylie y McDonald 2018

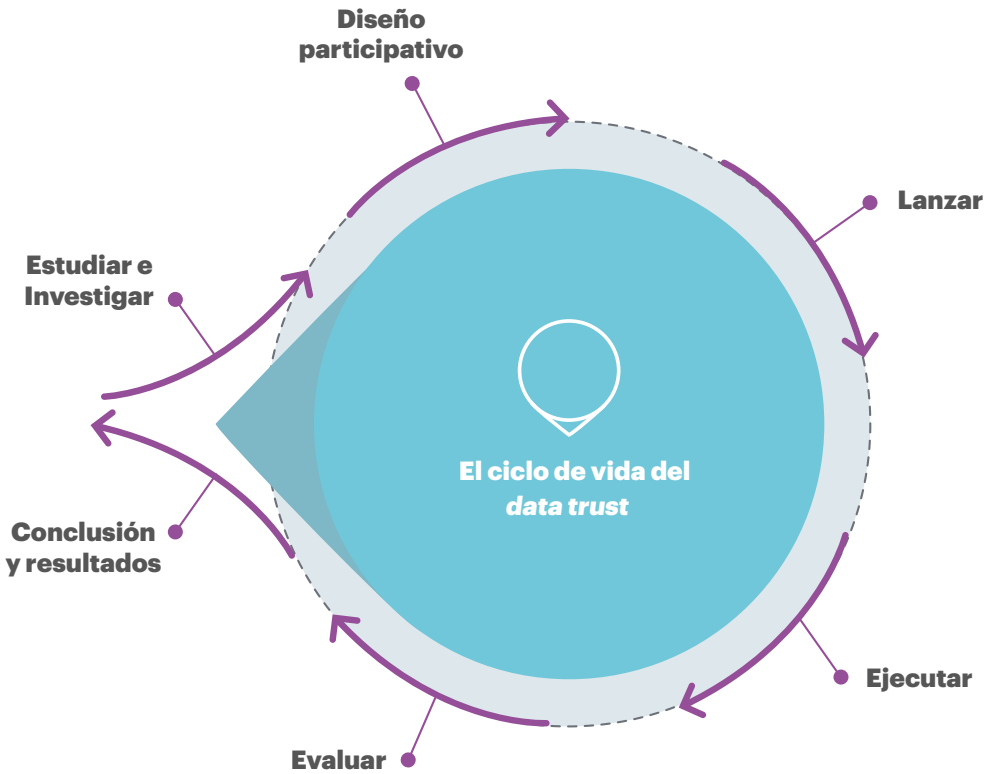
[47] Hardinges 2018

[48] Theodi.org 2018

[49] Reed et al. 2019

Los desafíos y oportunidades que plantea la implementación de estos tres programas piloto permitieron determinar un ciclo de vida del *data trust* que puede resultar útil para las entidades públicas que desean experimentar con este modelo de gobierno de datos. En él se muestran las actividades, los riesgos y las partes interesadas que deben participar en cada etapa del proceso de implementación.
Cabe señalar que la seguridad y la sostenibilidad son primordiales en este modelo de gobernanza de datos.

El ciclo de vida del *data trust*



Fuente de las imágenes: The odi.org 2018

Evaluaciones del impacto

Las "evaluaciones del impacto de la protección de datos" (data protection impact assessments DPIA, por sus siglas en inglés) son iniciativas voluntarias que suelen partir de organismos públicos centrados en el cumplimiento y el control en el sector de la salud. Con todo, implantar las DPIA a mayor escala podría tener implicaciones positivas en el diseño de sistemas algorítmicos y podría convertirse en una norma obligatoria, especialmente cuando se trata de aspectos éticos vinculados a datos personales confidenciales, y permitir explorar escenarios futuros probables sobre los que proponer recomendaciones de gobernanza para el presente.

Certificaciones

Las medidas voluntarias presentan nuevas oportunidades de llevar a la práctica la ética en forma de certificaciones dirigidas a los propios algoritmos o a las personas o procesos que intervienen en la toma de decisiones. Los problemas de equidad y discriminación podrían tenerse en cuenta en los criterios de certificación, así como la oportunidad de incentivar de manera proactiva la creación de algoritmos más controlables. El proyecto fAIr LAC es una oportunidad para desarrollar la capacitación local y la normativa en países latinoamericanos a través de la labor conjunta de empresas y gobiernos locales para ofrecer certificados de excelencia en IA responsable.

En esta sección hemos analizado los principales desafíos y oportunidades de la gobernanza ética de los datos identificados por los expertos del grupo de trabajo. La lista no es exhaustiva, ya que seguramente surgirán más elementos a medida que avance la digitalización y la IA. A medida que crece la preocupación por el uso y la gobernanza de los datos, las entidades públicas y privadas empiezan a mostrar un mayor compromiso a la hora de abordar los desafíos de la ética de datos y la privacidad digital. Sin embargo, se necesitan acciones concretas que vayan más allá del compromiso y garanticen la recopilación y el uso ético de datos, aspectos que deben ser prioritarios para los responsables de formulación de políticas en los próximos años. En la siguiente sección trataremos los factores que probablemente acaben determinando el panorama de la ética de los datos y exploraremos futuros probables que nos permitan proponer recomendaciones de gobernanza de datos para el presente.

3

Mirando hacia el futuro con la vista puesta en el presente

Diseño de futuros

La metodología utilizada en los grupos de trabajo de Digital Future Society se basa en la herramienta de diseño de futuros para facilitar el debate, el análisis colectivo y la anticipación estratégica frente a los grandes desafíos y oportunidades que podrían surgir en la próxima década.

El diseño de futuros crea un espacio donde idear recomendaciones de futuro válidas y plausibles a partir del debate y el análisis (desde múltiples perspectivas) de las principales tendencias e incertidumbres que impactan, y se prevé impactarán, en las tecnologías emergentes.

Este concepto no debe confundirse, utilizarse mal ni malinterpretarse como si su finalidad fuera la de "predecir el futuro". No se trata de predecir lo que sucederá en 2030, sino más bien aplicar el pensamiento colectivo a largo plazo y evitar el habitual sesgo retrospectivo al analizar el impacto de las tecnologías emergentes en la sociedad.

En esta sección se presentan tres escenarios que corresponden a tres marcos emotivos posibles: el optimista, el pragmático y el catastrófico. Cada uno de ellos imagina cómo será el mundo en 2030.

¿Por qué 2030?

Basar los escenarios de este informe en el horizonte temporal de 2030 permite a Digital Future Society presentar recomendaciones en un marco compartido que tenga en cuenta los distintos relatos internacionales existentes, en particular los Objetivos de Desarrollo Sostenible (ODS) de Naciones Unidas. 2030 es una referencia temporal que utilizan muchos otros gobiernos, organizaciones internacionales e iniciativas internacionales de entidades como el Foro Económico Mundial, el Banco Mundial y la Comisión Europea.

Nuestro objetivo es alentar a los responsables de formulación de políticas a basarse en el marco de los ODS para construir una visión común compartida de futuro o futuros deseables cuando se enfrenten a decisiones éticas y de gobernanza de datos, especialmente a la luz de los objetivos diseñados para promover instituciones más sólidas, educación de calidad, igualdad de género, trabajo decente, reducción de las desigualdades e innovación en las industrias y las infraestructuras. Mirar hacia delante y prever cómo podrían ser los posibles futuros de un mundo basado en datos y cómo podrían afectar a factores sociales, económicos y medioambientales nos permite articular desde ahora respuestas políticas orientadas a la acción.

Una observación sobre la construcción de escenarios

Este ejercicio parte del debate sobre los desafíos y las oportunidades actuales a los que deben responder las entidades públicas y privadas y se centra en crear consenso sobre la probabilidad y la magnitud de las incertidumbres que, según los expertos, tendrán un mayor impacto en los próximos años. El objetivo es anticipar acontecimientos que cambien la situación con el fin de presentar recomendaciones prácticas que permitan abordar los numerosos desafíos y oportunidades que plantean la ética y la gobernanza de los datos. Para los expertos participantes en el grupo de trabajo, los principales problemas a la hora de anticipar los desafíos de la próxima década a los que habrá que dar respuesta son la dicotomía entre datos y algoritmos pertenecientes a ciudadanos y datos y algoritmos propiedad de empresas y la dicotomía alta/baja participación social en cuestiones de ética de datos.

Escenario A: mis datos, mis reglas

La agenda de gobernanza de datos impulsada por ciudadanos comprometidos

Tras una serie de violaciones críticas de datos y escándalos de privacidad de alcance global, los ciudadanos, muy preocupados por los datos, disponen de mecanismos seguros de acceso y titularidad de los datos y algoritmos. Deseosa de debatir y actuar, la sociedad civil se ha organizado en grupos y movilizado contra entidades públicas y privadas que utilizan sus datos personales para su beneficio y han conseguido influir con éxito en los gobiernos para que implementen leyes que respalden este modelo. En este escenario los ciudadanos están plenamente capacitados ya que controlan totalmente cómo se utilizan sus datos y en qué medida sus vidas se ven afectadas por los algoritmos. Gracias a su gran capacidad de movilización y defensa de sus intereses, los ciudadanos intervienen decisivamente en un mundo basado en datos.

Más allá de las estrictas leyes de privacidad nacionales, existe un consenso internacional en torno a los derechos en materia de datos de los ciudadanos basado en la histórica legislación RGPD, cuyas «copias» se han aprobado en todo el mundo. El resultado es un mercado mucho más concentrado puesto que los ciudadanos tienen más poder sobre los algoritmos y son dueños de sus datos, lo que reduce las posibilidades de que algunas empresas recopilen y usen datos personales.

Este escenario ofrece varias oportunidades para que los gobiernos usen y regulen los datos de manera ética, no solo para mejorar los servicios públicos, sino también para dar ejemplo al sector privado. Al financiar la creación de algoritmos y aplicar principios éticos por defecto, los gobiernos podrían predicar con el ejemplo a través de iniciativas innovadoras de privacidad desde el diseño. El sector público también tiene la oportunidad de redefinir la relación entre entidades públicas y privadas y de fomentar la autonomía al reducir la concentración de datos y la propiedad de algoritmos en manos privadas.

Entre los desafíos a los que los gobiernos tendrán que enfrentarse en este escenario destacan los siguientes: encontrar formas de hacer efectiva la transparencia y readaptar las políticas a una ciudadanía muy comprometida que sigue responsabilizándolos de la recopilación y el uso ético de datos. Se necesitará más inversión pública para financiar entidades que lleven a cabo investigaciones imparciales sobre la ética de los datos y supervisión por parte de terceros.

Escenario B: vulnerabilidad por indiferencia

Aunque están consagradas por la ley, la ética y la privacidad de los datos se dan por sentadas

Este escenario se caracteriza por una especie de agotamiento frente a los datos. Si bien existe una legislación que atribuye la propiedad de los datos a los ciudadanos y los algoritmos son abiertos, los ciudadanos no entienden ni se preocupan por las consecuencias de la utilización de sus datos por parte de las empresas, lo que en la práctica supone una renuncia a los derechos digitales.

De nuevo, en este escenario la legislación RGPD se ha convertido en un punto de referencia internacional, incluso para los gobiernos previamente en desacuerdo de América del Norte y Asia. No solo han cambiado las actitudes políticas, sino que el cumplimiento y el cambio de paradigma respecto a la propiedad de los datos también se han convertido en la norma en el sector privado. En concreto, establecer la finalidad y el uso concreto de datos y minimizar su recopilación se han convertido en práctica comercial habitual. Como resultado, existe una mayor complejidad técnica, una mayor necesidad de control y los precios del software han aumentado. Las empresas más grandes y con más recursos para implementar normas de ética y privacidad de datos consiguen importantes ingresos y superan a las pequeñas empresas emergentes y pymes. Reducir los costes comerciales supone un gran desafío para los sectores público y privado en este escenario.

Otro reto que se plantea es el uso de datos para bienes sociales, que se vuelve más difícil debido a la «sobrerregulación». Los usuarios de la tecnología se centran en los beneficios personales a corto plazo, pero el papel de los ciudadanos sigue siendo pasivo. En este escenario, les corresponde a los gobiernos utilizar los datos para mejorar los servicios públicos de una manera ética y respetando, en primer lugar, la privacidad. Esto también puede verse como una oportunidad para que los gobiernos implementen políticas participativas de gobernanza de datos.

.

Escenario C: los datos, moneda de cambio en una sociedad mejor

Alta participación social y propiedad de los datos concentrada en grandes multinacionales

En este escenario, es la sociedad la que disfruta de los beneficios de los sistemas digitales. Los ciudadanos quieren saber quién tiene sus datos y cómo se utilizan. Se admite que un puñado de entidades públicas y privadas dominantes son las titulares de los datos y los recopilan activamente. Por lo general, las personas aceptan que los gobiernos y las empresas posean y usen sus datos personales, ya que todo forma parte de un marco regulatorio en materia de gobernanza de datos claro y bien aplicado.

Tras años de la creciente desconfianza en las empresas tecnológicas (el llamado *techlash*), los ciudadanos ahora exigen un uso más responsable de las plataformas digitales y de las redes sociales por parte de gobiernos y empresas. Los fuertes movimientos contra la falta de transparencia y el mal uso de los datos han llevado a un aumento en el número de demandas colectivas contra empresas que abusan de los datos y la privacidad de las personas. La explicabilidad, ahora requerida por ley, de los algoritmos ha hecho que la implementación de tecnologías digitales automatizadas sea más costosa.

Una concepción nueva y necesaria de la privacidad y la ética de los datos se ha afianzado en los negocios y en toda la sociedad. Las organizaciones desarrollan sus productos y servicios basándose en la privacidad desde el diseño para recopilar la menor cantidad de datos posible. Los ciudadanos como Sorine ejercen regularmente sus derechos sobre los datos a través de solicitudes de acceso y portabilidad. Los ciudadanos no solo pueden visitar una plataforma consolidada para ver qué empresas han recopilado sus datos, sino que también pueden cancelar y borrar transacciones no deseadas. Aunque parezca una labor titánica, es una herramienta técnica que juega un papel importante en la lucha contra el seguimiento encubierto, la recopilación y venta de metadatos y otras prácticas poco éticas de tratamiento de datos. También existe la opción de consultar a dónde han ido los datos o el valor obtenido por compartirlos o venderlos y la capacidad de defenderse e incluso de recibir una compensación, impuesta por un consejo global de ética de datos.

Aunque los gobiernos y las multinacionales tienen más difícil hacer un mal uso de los datos, la monetización aún está permitida y los mercados de datos han crecido en todo el mundo. Surgen nuevas oportunidades de crecimiento con la creación de nuevas economías de datos, mercados y fuentes de ingresos. Por otro lado, los gobiernos se enfrentan a obstáculos regulatorios a nivel supranacional, ya que coordinar una respuesta global con los desafíos de ética y privacidad de los datos resulta difícil, especialmente cuando se trata de lidiar con los monopolios transnacionales sobre cuestiones de propiedad y tratamiento de datos.

Unas pocas empresas con grandes volúmenes de datos y algoritmos en su poder tienen la oportunidad de desarrollar una amplia gama de productos más baratos, pero los responsables de formulación de políticas se enfrentan a desafíos a la hora de aplicar la normativa.


Code of
Conduct

Escenario D: los ganadores se lo llevan todo

Indiferencia social frente a los monopolios de datos

En este escenario, la concentración de datos alcanza su máximo en manos de lo que la futuróloga Amy Webb llama *The Big Nine*, o las nueve grandes: Amazon, Apple, Google, Facebook, IBM, Microsoft, Baidu, Tencent y Alibaba. No hay transparencia con respecto al uso de datos y las personas se muestran contentas con las plataformas digitales sin pensar mucho en la ética o la privacidad de los datos.

Aparte del ya obsoleto RGPD, los gobiernos de Europa u otros lugares no han hecho más por aumentar la alfabetización digital, la ética de los datos o la privacidad. La externalización de los servicios públicos es algo común, con aplicaciones digitales fáciles de usar y omnipresentes tanto en los servicios públicos como en los privados.

Incapaces de competir con los gigantes de datos, las tiendas locales y las pequeñas empresas han cerrado a un ritmo sin precedentes y ahora son cada vez más escasas, incluso en centros no digitales. Tras haber influido en la política directamente y a través de lobbies, las "nueve grandes" ahora presionan en la redacción de leyes y reglamentos para garantizar su dominio.

En este escenario, tanto los ciudadanos como el gobierno tienen un papel pasivo en la forma en que se utilizan los datos y la regulación está completamente en manos del sector privado. El poder de decisión sobre los datos se ha externalizado en el sector público, incluso el proceso electoral. La protección de la privacidad nace del contexto de los derechos de propiedad intelectual en lugar de los derechos humanos y cualquier forma de datos se considera propiedad de las multinacionales que los utilizan, no de los ciudadanos que los facilitan. Todo esto supone una importante barrera para los gobiernos que buscan mejorar los servicios públicos, ya que ahora carecen de acceso y no son titulares de los datos y deben apoyarse en empresas privadas.


0101

4

Del análisis a la acción

Hacia una mejor gobernanza de datos

Nuestra creciente dependencia en la tecnología y en sistemas basados en datos, en la esfera personal y pública, se ha traducido en una mayor inquietud respecto a la gobernanza de datos, especialmente en lo referente a la privacidad y la transparencia. El nuevo panorama de la ética de datos requiere un enfoque pluridimensional y multidisciplinario que aborde los desafíos y oportunidades descritos en la sección 2.

Conscientes de que el debate iniciado en este informe tendrá continuación, hemos establecido una serie de recomendaciones destinadas a servir de punto de partida para la gobernanza ética de los datos y, en general, para la construcción de futuros digitales más equitativos.

1. Predicar con el ejemplo

1.1 Priorizar la privacidad desde el diseño: hacia la autonomía moral de los ciudadanos digitales

Se entiende por autonomía moral el control sobre la forma en la que una persona se ve a sí misma, y es un derecho fundamental que debe respetarse en la misma medida tanto en el mundo digital como en el físico. Ante la mayor exigencia de transparencia sobre los usos dados a los datos que las personas proporcionan en Internet, los gobiernos tienen la oportunidad de generar confianza si comunican claramente sus acciones a los ciudadanos.

Para llevarlo a la práctica con carácter inmediato, los gobiernos pueden considerar agregar cuadros informativos (por ejemplo, qué hacemos con sus datos) en los sitios web públicos y animar a las entidades privadas que quieran trabajar con ellos a hacer lo mismo. Las entidades públicas deben esforzarse en prestar servicios públicos de acuerdo con los principios de privacidad desde el diseño.[50] Los gobiernos de Estonia, Austria e India están implementando características de diseño y marcos regulatorios basados en principios y prácticas que tienen como objetivo garantizar la privacidad de los datos en sus sistemas nacionales de identificación digital.[51]

[50] Véase Anexo II

[51] Grupo del Banco Mundial 2018

1.2 Optar sistemáticamente por el código abierto

Las políticas de datos abiertos son una forma de promover el uso ético de los datos en la prestación de servicios públicos. Aunque las empresas privadas no estén obligadas a compartir cómo recopilan datos y diseñan algoritmos, sí pueden promover la confianza siendo transparentes sobre las vulnerabilidades conocidas en el software y comunicando las infracciones de datos puntualmente. También pueden dirigir otros esfuerzos de cooperación digital basados en valores para abordar desafíos éticos y de transparencia específicos.

Los responsables de formulación de políticas pueden predicar con el ejemplo utilizando alternativas a las plataformas dominantes de recolección de datos. La concentración de datos se puede reducir mediante el uso de soluciones y servicios alternativos, como los enumerados por el grupo de expertos danés Data Ethics. La ciudad de Barcelona es un ejemplo práctico de cómo aplicar esta recomendación con sus herramientas para establecer políticas Estándares Éticos Digitales.[53]

1.3 Experimentar con nuevos modelos de gobernanza de datos

Los gobiernos deben colaborar con la industria, las entidades de la sociedad civil y los investigadores para probar nuevos modelos de gobernanza de datos, por ejemplo *data trusts*, que mejoren los modelos de privacidad basados en el consentimiento, particularmente en los departamentos que usan o planean usar sistemas automatizados de toma de decisiones.

Al experimentar con nuevos modelos de gobernanza de datos, los responsables de formulación de políticas deben aspirar a un enfoque sostenible, voluntario y participativo de la recopilación y el uso de datos personales a medida que implementan tecnologías basadas en datos para la prestación o la mejora de los servicios públicos. Abrir el ámbito tecnológico a la participación ciudadana al crear algoritmos puede garantizar un enfoque más diverso a la vez que ético del diseño de algoritmos y el despliegue de la IA.

[52] Dataethics.eu 2018

[53] Barcelona.cat 2018

2. Llevar a la práctica la ética a través de la rendición de cuentas

2.1 Aplicar mecanismos de rendición de cuentas al uso poco ético de datos

El mal uso de los datos por parte de entidades públicas y privadas debe tener consecuencias. Los esfuerzos europeos por liderar cambios regulatorios que conlleven prácticas más estrictas de protección de datos y privacidad desde el diseño han logrado crear concienciación sobre la ética de los datos a nivel mundial. Sin embargo, la implementación de mecanismos de rendición de cuentas sólidos sigue siendo un reto.

Una iniciativa que podría implementarse de inmediato es la creación y el mantenimiento de una lista pública de vendedores de datos. Algo tan simple como una lista de empresas que compran y usan información personal podría contribuir en gran medida a subir el listón y propiciar un comportamiento más consciente en materia de privacidad y una gobernanza más responsable de los datos.

Los responsables de formulación de políticas también podrían recoger y publicar una serie de casos prácticos que demuestren cómo su gobierno o departamento lleva a la práctica la ética de los datos, junto con un plan de revisión y actualización periódica. En casos de despliegue de IA, el documento debe explicar claramente cuál es la gravedad de las repercusiones de cada sistema, así como indicar qué persona tiene el control del sistema.

2.2 Crear condiciones favorables para un cambio en el sector privado hacia el desarrollo de la tecnología ética

Los gobiernos tienen un papel clave en la creación de condiciones en las que la gobernanza ética de los datos no reste competitividad a las pequeñas y medianas empresas. Los responsables de formulación de políticas deben considerar la competitividad de su sector tecnológico local e introducir mecanismos y medidas que apoyen el crecimiento de manera ética. La regulación debe ser lo suficientemente flexible para evitar sofocar el emprendimiento y la innovación y a la vez propiciar nuevas posibilidades que lleven a los consumidores a valorar la confianza. El apoyo del sector público al cumplimiento, por parte del sector privado, de las regulaciones en materia de datos y los principios éticos, por ejemplo a través de ayudas a las empresas que innoven con datos éticamente certificados, podría contribuir positivamente a este cambio.

3. Adoptar un enfoque inclusivo y transparente

Cuando hablamos de gobernanza transparente de los datos no nos referimos simplemente a comunicar la propiedad o el consentimiento de los datos, sino más bien a cuándo, cómo y por qué las entidades públicas y privadas utilizan los datos. El grupo de trabajo acordó que las entidades públicas y privadas tienen la obligación de ser transparentes, especialmente al utilizar datos de los ciudadanos para la prestación de servicios públicos.

3.1 Abordar las brechas en la alfabetización de datos mediante el desarrollo y la distribución de programas educativos para usuarios *online y offline*

En colaboración con las partes interesadas del sector público y privado, los gobiernos deberían emprender una iniciativa de educación pública centrada en la ética y la privacidad de los datos para mejorar la alfabetización en materia de datos. Dicho programa debe tener en cuenta la búsqueda, por parte de las personas, de una personalidad pública propia y la forma de ejercer sus derechos digitales, además de garantizar una disponibilidad inclusiva (debe estar disponible tanto en línea como fuera de línea). Al finalizar el programa, los usuarios deberían comprender qué hacen las entidades con sus datos y cómo garantizar que su gemelo digital tenga autonomía moral. Finlandia es un ejemplo instructivo en este caso con su curso gratuito en línea «Elementos de IA», completado por más de 10.000 personas. El país prevé lograr que el 1% de su población realice el curso, es decir 55.000 ciudadanos.[54]

3.2 Promover una fuerza laboral de IA diversa e interdisciplinaria

La calidad del resultado y la integridad ética de un algoritmo dependen de que se garantice que el sesgo inherente de los programadores no se haya transferido al código. Un grupo diverso de programadores reduce el riesgo de incorporar sesgo a los algoritmos y ofrece resultados más justos y de mayor calidad.

Para alcanzar la paridad representativa y garantizar que los derechos digitales se consideren desde múltiples perspectivas, es crucial promover una fuerza laboral diversa que incluya grupos subrepresentados (especialmente en términos de género, raza y economía). Los responsables de formulación de políticas también tienen el cometido de garantizar un enfoque interdisciplinario que aumente la transparencia y la responsabilidad. Los abogados, diseñadores de interfaces, sociólogos y especialistas en ética deben trabajar junto con los ingenieros informáticos si queremos llevar la ética y el estado de derecho al diseño de sistemas algorítmicos.

[54] Decker 2019

4. Una llamada a la acción

A lo largo de la historia, las sociedades siempre han logrado actuar de una u otra manera cuando se enfrentaban a grandes riesgos de alcance mundial. Las entidades públicas y privadas han tenido que adaptarse a estos requisitos no solo con una evaluación de riesgos específica y una gestión responsable, sino innovando y evolucionando de nuevas maneras. Tendrán que hacer lo mismo en un entorno saturado de datos. A través de nuevas leyes, normas globales, sistemas de responsabilidad formal en los que los ciudadanos puedan confiar y una adaptación cultural lenta pero constante, podemos continuar alcanzando nuevos niveles de conciencia, educación, alfabetización en materia de datos y una mejor gobernanza cuando se trata de diseñar e implementar tecnologías basadas en datos.

Concluimos este informe desafiando a los responsables de formulación de políticas a probar las recomendaciones propuestas en el presente documento, ya sea a través de entornos limitados, programas piloto, períodos de prueba o creación de prototipos. Solo a través de la experimentación y la política basada en los hechos podremos pasar de la reflexión a la acción en nuestra búsqueda de un futuro digital más equitativo e inclusivo.

Referencias y agradecimientos

Referencias

Algorithm Watch. (2018). *Automating Society Taking Stock of Automated Decision-Making in the EU*. Disponible en: https://algorithmwatch.org/wp-content/uploads/2019/02/Automating_Society_Report_2019.pdf

Barcelona.cat. (n.d.). *Ethical Digital Standards: Executive Summary*. [online] Disponible en: https://www.barcelona.cat/digitalstandards/en/data-management/0.1/summary

Building Ethics Into Privacy Frameworks For Big Data and AI. (2018). [PDF] United Nations Global Pulse and the International Association of Privacy Professionals. Disponible en: https://iapp.org/media/pdf/resource_center/BUILDING-ETHICS-INTO-PRIVACY-FRAMEWORKS-FOR-BIG-DATA-AND-AI-UN-Global-Pulse-IAPP.pdf

Cavoukian, A. (n.d.). *Privacy by Design: The Seven Foundational Principles*. [PDF] Privacy and Big Data Institute. Disponible en: https://www.ryerson.ca/content/dam/pbdce/seven-foundational-principles/The-7-Foundational-Principles.pdf

Dataethics.eu. (2018). *Data Ethics Tools for Companies and Organisations - Dataethical Thinkdotank*. [online] Disponible en: https://dataethics.eu/tools/

Delcker, J. (2019). *Finland's grand AI experiment*. [online] POLITICO. Disponible en: https://www.politico.eu/article/finland-one-percent-ai-artificial-intelligence-courses-learning-training

Doctorow, C. (2019). *Adversarial Interoperability: Reviving an Elegant Weapon From a More Civilized Age to Slay Today's Monopolies*. [online] Electronic Frontier Foundation. Disponible en: https://www.eff.org/deeplinks/2019/06/adversarial-interoperability-reviving-elegant-weapon-more-civilized-age-slay

Edwards, L. and Veale, M. (2017). Slave to the Algorithm? *Why a Right to Explanation is Probably Not the Remedy You are Looking for. SSRN Electronic Journal*.

Figure Eight. (2019). *The Artificial Intelligence (AI) Glossary*. [online] Disponible en: https://www.figure-eight.com/resources/the-artificial-intelligence-glossary

Floridi, L. and Taddeo, M. (2016). *What is data ethics?* Philosophical Transactions A, Royal Society Publishing. [PDF] Disponible en: https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2016.0360

Foro Económico Mundial. (2019). The Global Risks Report. 14ª ed. [PDF] Ginebra: Foro Económico Mundial. Disponible en: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Furseth, J. (2019). *The big picture: What we lost in the wilderness years of photo storage*. [online] Findingctrl.nesta.org.uk. Disponible en: https://findingctrl.nesta.org.uk/in-the-wilderness-years-of-photo-storage

Grupo Banco Mundial. (2018). Privacy by Design: Current Practices in Estonia, India, and Austria. Identification of Development (ID4D). [PDF] Disponible en: https://id4d.worldbank.org/sites/id4d.worldbank.org/files/PrivacyByDesign_112918web.pdf

Hardinges, J. (2018). *What is a data trust? – The ODI*. [online] Theodi.org. Disponible en: https://theodi.org/article/what-is-a-data-trust/

Hardinges, J. and Wells, P. (2018). *Defining a data trust*. [online] Theodi.org. Disponible en: https://theodi.org/article/defining-a-data-trust/

Iapp.org. *General Data Protection Regulation*. [online] Disponible en: https://iapp.org/resources/article/general-data-protection-regulation/#

Ingold, D. and Soper, S. (2016). *Amazon Doesn't Consider the Race of Its Customers. Should It?*. [online] Bloomberg.com. Disponible en: https://www.bloomberg.com/graphics/2016-amazon-same-day/

Inside Privacy. (2019). Thailand Adopts Personal Data Protection Act. [e online Disponible en: https://www.insideprivacy.com/data-privacy/thailand-passes-personal-data-protection-act/

Katwala, A. (2018). *How to make algorithms fair when you don't know what they're doing*. [online] Wired.co.uk. Disponible en: https://www.wired.co.uk/article/ai-bias-black-box-sandra-wachter

Liao, T. (2018). *China Publishes National Standard for Personal Data Protection*. [online] Morganlewis.com. Disponible en:: https://www.morganlewis.com/pubs/china-publishes-national-standard-for-personal-data-protection

McNamara, A., Smith, J. and Murphy-Hill, E. (2018). Does ACM's code of ethics change ethical decision making in software development?. *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering - ESEC/FSE 2018*.

Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S. and Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2).

Molla, R. (2019). *Mary Meeker's most important trends on the internet*. [online] Vox. Disponible en: https://www.vox.com/recode/2019/6/11/18651010/mary-meeker-internet-trends-report-slides-2019

Mulgan, G. and Straub, V. (2019). *The new ecosystem of trust*. [online] nesta. Disponible en: https://www.nesta.org.uk/blog/new-ecosystem-trust/

Müller-Eiselt, R. (2018). *An Ethics for Algorithmists – Lessons Learned from Effective Professional Ethics*. [online] Ethics of Algorithms. Disponible en: https://ethicsofalgorithms.org/2018/09/24/an-ethics-for-algorithmists-lessons-learned-from-effective-professional-ethics

Nytimes.com. (2019). *The New Terminology for Privacy*. [online] Disponible en: https://www.nytimes.com/interactive/2019/04/10/opinion/internet-privacy-terms.html

Panel de Alto Nivel del Secretario General de las Naciones Unidas sobre Cooperación Digital. (2019). La era de la interdependencia digital. [PDF] Disponible en: https://www.un.org/sites/www.un.org/files/uploads/files/es/HLP%20on%20Digital%20Cooperation%20Report%20Executive%20Summary%20-%20ES%20.pdf

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.

Plataforma CGAIR para Big Data en Agricultura. (2019). Plataforma CGAIR para Big Data en Agricultura. [online] Disponible en: https://bigdata.cgiar.org/

Powles, J. and Nissenbaum, H. (2018). *The Seductive Diversion of 'Solving' Bias in Artificial Intelligence*. [online] Medium.Disponible en: https://medium.com/s/story/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53

Privacy and Data Protection Policy 2018 - Kenya. (2018). [PDF] The Government of Kenya. Disponible en: http://www.ict.go.ke/wp-content/uploads/2018/08/Kenya-Data-Protection-Policy-2018-15-8-2018.pdf

Reed, C., BPE Solicitors, Pinsent Masons (2019). *Data trusts: legal and governance considerations*. [PDF] Disponible en: http://theodi.org/article/data-trusts-legal-report/

Salleh Rahaman, A. (2015). *Data Protection Policy*. [PDF] E-Government National Centre of Brunei. Disponible en: http://www.information.gov.bn/PublishingImages/SitePages/New%20Media%20and%20IT%20Unit/Data%20Protection%20Policy%20V.2.2.pdf

Schermer, B. (2011). The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, 27(1), pp.45-52.

Theodi.org. (2018). *UK's first 'data trust' pilots to be led by the ODI in partnership with central and local government – The ODI*. [online] Disponible en: https://theodi.org/article/uks-first-data-trust-pilots-to-be-led-by-the-odi-in-partnership-with-central-and-local-government/

Turilli, M. y Floridi, L. (2009). The ethics of information transparency. *Ethics and Information Technology*, 11(2), pp.105-112.

van den Hoven, J. (2008). *Information technology, privacy, and the protection of personal data, in Information technology and moral philosophy*, J. Van Den Hoven and J. Weckert (eds.), Cambridge: Cambridge University Press, pp. 301–322.

Vincent, J. (2019). *AI is worse at identifying household items from lower-income countries*. [online] The Verge. Disponible en: https://www.theverge.com/2019/6/11/18661128/ai-object-recognition-algorithms-bias-worse-household-items-lower-income-countries

VPRO (2018). *Algorithms Rule Us All*. [video] Disponible en: https://www.youtube.com/watch?v=NFF_wj5jmiQ

Warren, S. and Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), p.193.

Webb A., Giralt, E., Palatucci, M. & Perez, K. (2019). Tech Trends Report. [PDF] Future Today Institute.

Wendy, D. & Pesenti, J. (2017). Growing the Artificial Intelligence Industry in the UK. [PDF] GOV.UK. Disponible en: https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk

Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, V., Myers West, S., Richardson, R., Schultz, J. and Schwartz, O. (2018). AI Now Report 2018. [PDF] New York: AI Now Institute.Disponible en: https://ainowinstitute.org/AI_Now_2018_Report.pdf

Agradecimientos

Autor principal

- **Adriana Díaz** – Investigadora, Digital Future Society Think Tank

Coautores

- **Nicole Harper** – Editora, Digital Future Society Think Tank

Colaboradores expertos

Este informe ha sido posible gracias a las ideas y aportaciones de los siguientes expertos:

- **Aimee van Wynsberghe** – Co-Director, Foundation for Responsible Robotics and Assistant Professor, Ethics and Philosophy of Technology, Delft University of Technology
- **Arran Riddle** – Director de contenido de políticas y normativas, GSMA
- **Artur Serra** – Subdirector, i2cat and Leadership Member, European Network of Living Labs
- **Atia Cortés** – Ingeniera informático e investigadora en inteligencia artificial, Universidad Politécnica de Cataluña
- **César Buenadicha** – Chief Discovery Officer, Banco Interamericano de Desarrollo
- **Fabro Steibel** – Director ejecutivo, Instituto de Tecnología y Sociedad de Río de Janeiro
- **Grace Mutung'u** – Analista de políticas, Kenya ICT Action Network (KICTANet)
- **Jade Nester** – Directora de política del consumidor, GSMA
- **Joan Roses** – Editor, Collateralbits
- **Lavinia Marin** – Profesora de Ética y Filosofía de la Tecnología, Universidad Tecnológica de Delft
- **Marc Blasi** – Gerente de proyectos de Big Data, CaixaBank
- **Marc Torrent** – Director de Big Data Analytics, Eurecat y Director del Big Data Center of Excellence Barcelona
- **Sandra Álvaro** – Investigadora, Centre de Cultura Contemporània de Barcelona

- **Tarek Besold** – Artificial Intelligence Lab Lead, Alpha Health and Chair, German National Standards Working Group on Artificial Intelligence
- **Ulises Cortés** – Director científico, High-Performance Artificial Intelligence, Barcelona Supercomputing Center
- **Victoria Anderica** – Directora del Proyecto de Transparencia, Ayuntamiento de Madrid

Equipo de Think Tank de Digital Future Society

Se agradece el trabajo editorial y las aportaciones de las siguientes miembros del equipo:

- **Carina Lopes** – Directora, Digital Future Society Think Tank

Citación

Por favor cite este informe de la siguiente manera:

- Digital Future Society. (2019). Hacia una mejor gobernanza de datos para todos: Ética y privacidad de los datos en la era digital. Barcelona, España.

Apéndices

Anexo I: Inventario global de ética de datos marcos y principios

No hay escasez de sugerencias sobre cómo las tecnologías basadas en datos deben ser gobernadas éticamente, como lo demuestra esta lista no exhaustiva. Desde iniciativas gubernamentales hasta esfuerzos supranacionales, solo en los últimos tres años hemos visto un número creciente de principios, declaraciones, compromisos voluntarios y propuestas de marco para el uso ético de los datos y la IA.

Organización	Año	Principios	Sector	Fuente
Datenschutzkonferenz	Abr 2019	Declaración de Hambach sobre Inteligencia Artificial (en alemán)	Privado	Algorithm Watch
Comisión Europea (AI-HLEG)	Abr 2019	Pautas de ética para una IA confiable	Público	Instituto Rathenau
Bundesverband KI	Mar 2019	Certificado KI (en alemán)	Privado	Algorithm Watch
Oficina del Comisionado de Información (ICO)	Mar 2019	Blog del marco de auditoría de IA	Público	Gobierno del reino Unido
Google	Ene 2019	Gobernanza de la IA	Privado	Instituto Rathenau
Smart Dubai	Dic 2018	Ética y principios de la inteligencia artificial	Público	Algorithm Watch
Atomium – EISMD (AI4People)	Nov 2018	Marco ético de AI4People para una buena sociedad de IA: Oportunidades, riesgos, principios, y recomendaciones	ONG	Algorithm Watch

Organización	Año	Principios	Sector	Fuente
Grupo danés de expertos en ética de datos (DATAETIK)	Nov 2018	Datos en beneficio de las personas	Público	Algorithm Watch
DataforGood	Nov 2018	Juramento hipocrático para el científico de datos (en francés)	Privado	Algorithm Watch
Banco Mundial	Nov 2018	Privacidad por diseño: prácticas actuales en Estonia, India y Austria.	Banco Multilateral de Desarrollo	El Banco Mundial
CIGREF	Oct 2018	Ética Digital	Privado - Público	Algorithm Watch
Comisionado de Privacidad y Jefe de Administración de Datos del Gobierno, Nueva Zelanda	Oct 2018	Principios para el uso seguro y efectivo de datos y analítica	Público	Gobierno de Nueva Zelanda
The Public Voice	Oct 2018	Pautas universales para la inteligencia artificial	NGOs	Instituto Rathenau
Asociación de Computación Maquinaria - Consejo de Políticas Públicas de los Estados Unidos	Sep 2018	Código Ético y de Conducta Profesional	Privado	Instituto Rathenau
Comisión Europea	Sep 2018	Código de prácticas sobre desinformación	Público	Algorithm Watch
IBM	Sep 2018	Ética para la IA: Una guía práctica para diseñadores y desarrolladores	Privado	Instituto Rathenau

Organización	Año	Principios	Sector	Fuente
SAP	Sep 2018	Principios rectores para la IA	Privado	Instituto Rathenau
Deutsche Telekom	Ago 2018	Pautas de ética digital sobre IA	Privado	Algorithm Watch
Amnistía Internacional y Access Now	Jul 2018	La Declaración de Toronto: Proteger el derecho a la igualdad y la no discriminación en los sistemas de aprendizaje automático	ONG	Rathenau Institut/ Algorithm Watch
Centro para la Innovación en Gobernanza Internacional (CIGI)	Jul 2018	Hacia un marco del G20 para la inteligencia artificial en el lugar de trabajo	Público	Algorithm Watch
Google	Jun 2018	Inteligencia artificial en Google: Nuestros principios	Privado	Instituto Rathenau
Fundación Bertelsmann, iRights.lab	May 2018	Algo.Rules	Privado	Algorithm Watch
Asociación sobre IA	Abr 2018	Preceptos	Privado - ONG	Instituto Rathenau
Cámara de los Lores del Reino Unido	Abr 2018	IA en el Reino Unido: ¿Listo, dispuesto y capaz?	Público	Instituto Rathenau
Cédric Villani, matemático y miembro del Parlamento francés	Mar 2018	Para una inteligencia artificial significativa: Hacia una estrategia francesa y europea	Público	Instituto Rathenau
Grupo europeo de ética de la ciencia y de las nuevas tecnologías	Mar 2018	Declaración sobre Inteligencia Artificial, Robótica y Sistemas 'Autónomos'	Público	Instituto Rathenau

Organización	Año	Principios	Sector	Fuente
Bitkom	Feb 2018	Recomendaciones para el uso responsable de la inteligencia artificial y responsabilidad digital corporativa de decisiones automatizadas, y toma de decisiones (en alemán)	Privado	Algorithm Watch
Cumbre Mundial del Gobierno 2018 (Dubai)	Feb 2018	Informe resumido 2018 (IA)	Público	Instituto Rathenau
Microsoft	Feb 2018	El futuro calculado	Privado	Instituto Rathenau
Telefonica	Feb 2018	Principios de IA de Telefónica	Privado	Instituto Rathenau
Ética de datos	Dic 2017	Principios de ética de datos	Privado	Algorithm Watch
IEEE	Dic 2017	Diseño éticamente alineado	Privado	Instituto Rathenau
Consejo de la Industria de Tecnología de la Información	Nov 2017	Principios de política de AI ITI	Privado	Instituto Rathenau
UNI Global Union	Nov 2017	Los 10 principios principales para la inteligencia artificial ética	ONG	Instituto Rathenau
Universidad de Montreal - Foro sobre el desarrollo socialmente responsable de la IA	Nov 2017	La Declaración de Montreal para un desarrollo responsable de la inteligencia artificial: Un proceso participativo	Privado	Instituto Rathenau

Organización	Año	Principios	Sector	Fuente
IBM	Oct 2017	Responsabilidad de datos de IBM	Privado	Instituto Rathenau
Future of Life Institute	Ago 2017	Principios IA de Asilomar	Privado - ONG	Instituto Rathenau
Ministerio Federal de Transporte y Digital Comité de Ética de Infraestructura	Jun 2017	Conducción automatizada y conectada (en alemán)	Público	Algorithm Watch
Centro para la Democracia y la Tecnología (CDT)	May 2017	Decisiones digitales	Público	Algorithm Watch
Asociación para Maquinaria de Computación Consejo de Políticas Públicas de los Estados Unidos	Ene 2017	Declaración sobre aransparencia algorítmica y rendición de cuentas	Privado	Rathenau Instituut/ Algorithm Watch
Equidad, responsabilidad y transparencia en el aprendizaje automático	Nov 2016	Principios para algoritmos responsables y una declaración de impacto social para algoritmos	Privado	Algorithm Watch
Accenture	Jun 2016	Principios universales de ética de datos	Privado	Algorithm Watch
Bitkom	Sep 2015	Pautas para aplicaciones de big data (en alemán	Privado	Algorithm Watch
Grupo de trabajo de ingeniería crítica	Oct 2011	El manifiesto de ingeniería crítica	Privado	Algorithm Watch

Anexo II: Privacidad por núcleo de diseño

Desarrollado por la Dra. Ann Cavoukian en la década de 1990, Privacy by Design es un marco que aborda los efectos sistémicos y en constante crecimiento de las tecnologías de la información y comunicación, las prácticas comerciales y los sistemas de datos en red a gran escala. Siete principios básicos informan sobre la base de once prácticas de información justas, las cuales se enumeran a continuación.[55]

- **Principio 1:** Proactivo no reactivo: preventivo no correctivo
- **Principio 2:** Privacidad como configuración predeterminada
- **Principio 3:** Privacidad integrada en el diseño
- **Principio 4:** Funcionalidad completa: suma positiva, no suma cero
- **Principio 5:** Seguridad de extremo a extremo: protección completa del ciclo de vida
- **Principio 6:** Visibilidad y transparencia: mantenlo abierto
- **Principio 7:** Respeto a la privacidad del usuario: manténgalo centrado en el usuario

Once prácticas de información justas	
Especificación del propósito	Los propósitos para los cuales se recopilan, utilizan, retienen y divulgan la información personal se comunicarán a la persona (sujeto de los datos) en el momento en que se recopila la información o antes. Los propósitos específicos deben ser claros, limitados y relevantes a las circunstancias.
Limitación de recopilación	La recopilación de información personal debe ser justa, legal y limitada a la que sea necesaria para los fines especificados.
Minimización de datos	La recopilación de información de identificación personal debe mantenerse al mínimo estricto. El diseño de programas, tecnologías de información y comunicaciones, y sistemas debe comenzar con interacciones y transacciones no identificables, como valor predeterminado. Siempre que sea posible, se debe minimizar la identificación, la observabilidad y la vinculación de la información personal.
Limitación de uso, retención y divulgación	El uso, retención y divulgación de información personal se limitará a los fines relevantes identificados para el individuo, para lo cual él o ella ha dado su consentimiento, excepto cuando la ley lo requiera. La información personal se conservará solo el tiempo que sea necesario para cumplir con los propósitos establecidos, y luego se destruirá de forma segura.

[55] Grupo del Banco Mundial 2018

Once prácticas de información justas	
Seguridad	Las entidades deben asumir la responsabilidad de la seguridad de la información personal (generalmente proporcional al grado de sensibilidad) a lo largo de todo su ciclo de vida, de acuerdo con los estándares que han sido desarrollados por reconocidos organismos de desarrollo de estándares.
Responsabilidad	La recopilación de información personal conlleva un deber de cuidado para su protección. La responsabilidad de todas las políticas y procedimientos relacionados con la privacidad deben documentarse y comunicarse según corresponda, y asignarse a un individuo específico. Al transferir información personal a terceros, se garantizará una protección de privacidad equivalente a través de medios contractuales u otros.
Apertura	La apertura y la transparencia son clave para la rendición de cuentas. La información sobre las políticas y prácticas relacionadas con la gestión de la información personal se pondrá a disposición de las personas.
Consentimiento	Se requiere el consentimiento libre y específico del individuo para la recopilación, uso o divulgación de información personal, y conforme lo autorice la ley. Cuanto mayor sea la sensibilidad de los datos, más clara y específica será la calidad del consentimiento requerido. El consentimiento puede ser retirado en una fecha posterior.
Precisión	La información personal será tan precisa, completa y actualizada como sea necesaria para cumplir con los propósitos especificados.
Acceso	A las personas se les proporcionará acceso a su información personal y estas serán informadas de sus usos y divulgaciones. Las personas deberán poder cuestionar la precisión e integridad de la información y modificarla según corresponda.
Cumplimiento	Las organizaciones deben establecer mecanismos de reclamo y reparación, y comunicar información sobre ellos al público, incluyendo cómo acceder al siguiente nivel de apelación.


Digital
Future Society